MATHEMATICS OF COMPUTATION
VOLUME 39, NUMBER 159
JULY 1982, PAGES 255–300

Strong Primality Tests That Are Not Sufficient

By William Adams and Daniel Shanks

Abstract. A detailed investigation is given of the possible use of cubic recurrences in primality tests. No attempt is made in this abstract to cover all of the many topics examined in the paper. Define a doubly infinite set of sequences $A(n)$ by

$$A(n+3) = rA(n+2) - sA(n+1) + A(n)$$

with $A(-1) = s$, $A(0) = 3$, and $A(1) = r$. If n is prime, $A(n) \equiv A(1) \pmod{n}$. Perrin asked if any composite satisfies this congruence if $r = 0$, $s = -1$. The answer is yes, and our first example leads us to strengthen the condition by introducing the "signature" of n:

$$A(-n-1), A(-n), A(-n+1), A(n-1), A(n), A(n+1)$$

mod n. Primes have three types of signatures depending on how they split in the cubic field generated by $x^3 - rx^2 + sx - 1 = 0$. Composites with "acceptable" signatures do exist but are very rare. The S-type signature, which corresponds to the completely split primes, has a very special role, and it may even be that I and Q type composites do not occur in Perrin's sequence even though the I and Q primes comprise 5/6ths of all primes. $A(n) \pmod{n}$ is easily computable in $O(\log n)$ operations. The paper closes with a p-adic analysis. This powerful tool sets the stage for our [12] which will be Part II of the paper.

1. A Certain Third-Order Recurrence. R. Perrin [1] defined the sequence

$$A(1) = 0, \quad A(2) = 2, \quad A(3) = 3, \quad A(n+3) = A(n) + A(n+1), \tag{1}$$

and observed that

$$n \mid A(n) \tag{2}$$

if n is prime. He found no composite n that satisfies (2) although he searched for one over a large range; Malo [2] and Escott [2a] discussed Perrin's sequence but neither obtained such a composite. Much later, Jarden [3] discussed (1) and related sequences but he also found no such composite.

We learned of the problem from S. Haber who told us that there is none up to 140,000. We rather quickly found that

$$n = 271441 = 521^2 \tag{3}$$

does satisfy (2), and we first indicate the considerations that led us to this composite: The recurrence (1) is reversible, and we have

$$A(0) = 3, \quad A(-1) = -1, \quad A(-2) = 1, \quad A(-3) = 2, \ldots .$$

We rewrite (2) as

$$A(n) \equiv A(1) \pmod{n}, \tag{4}$$

Received August 28, 1981.
1980 *Mathematics Subject Classification.* Primary 10A05, 10A25, 10A35, 12A30.

0025-5718/82/0000-0068/$13.00

and now add

$$A(-n) \equiv A(-1) \pmod{n}, \tag{5}$$

which is equally true if n is prime. We prove this later, deducing (4) and (5) from results valid for much more general sequences.

One finds that

$$A(-29) = A(-11) = A(-7) = A(-1) = -1, \tag{6}$$

so for these three primes we have not only congruence but even equality. Associated with (6) we find that (5) is satisfied by $n = 7^2$, 11^2, and 29^2. This does suggest that

$$p^2 \mid A(p^2) \tag{7}$$

probably holds for one or more primes p, but obviously the corresponding relation

$$A(p) = A(1) = 0 \tag{8}$$

does not hold for any p since $A(n)$ increases monotonically if $n > 0$.

But we do not need the full strength of (8) to obtain (7). One readily notes empirically, and we prove it below (again, under more general conditions), that

$$A(p^2) \equiv A(p) \pmod{p^2}, \qquad A(-p^2) \equiv A(-p) \pmod{p^2}. \tag{9}$$

The second congruence here enables us to deduce

$$A(-p^2) \equiv A(-1) \pmod{p^2} \quad \text{from} \quad A(-p) = A(-1)$$

merely by replacing the $A(-p)$ in (9) by $A(-1)$.

We can therefore obtain (7) if we can find an $A(p)$ not only divisible by p but also by p^2. Heuristically, the probability of such a p equals $1/p$, and since

$$\sum \frac{1}{p} \text{ diverges to } +\infty,$$

we actually expect infinitely many such p. However, they should be very sparse, since the manner of this divergence suggests that

$$\log \log p_n \sim n$$

if p_n is the nth example. In any case, $p_1 = 521$ (we know of no others), and so (9) implies that $p = 521$ satisfies (7).

Now we come to a critical point in the investigation. The designation of 521 as p_1 implies that $n = 7^2$, 11^2, and 29^2 fail to satisfy (4) although they do satisfy (5). Conversely, $n = 521^2$ satisfies (4) and fails to satisfy (5), since one computes

$$A(-521) \equiv 154736 = 297 \cdot 521 - 1 \pmod{521^2},$$

and then uses (9).

Besides $n = 7^2$, 11^2, and 29^2, one finds that $n = 7 \cdot 11$, $7 \cdot 29$, and $11 \cdot 29$ satisfy (5) and fail to satisfy (4). Therefore, we strengthen our requirements and ask if there is a composite c where

$$c \mid A(c) \quad \textit{and} \quad c \mid A(-c) + 1 \tag{10}$$

are true *simultaneously*. If, as suggested in [1], [2], even the first condition is rarely satisfied, then composite solutions of (10) should be very rare indeed.

Happily, in the algorithm that we develop in Section 5, it requires no extra computation to evaluate $A(n)$ and $A(-n)$ at the same time. *Au contraire*; when n is

large it is actually much *faster* to evaluate them together. If we were to compute

$$A(n) \pmod m \quad \text{or} \quad A(-n) \pmod m$$

directly from (1), then that would require $O(n)$ operations. Our algorithm takes only $O(\log n)$ operations and gives us the sextet

(11) $\quad A(-n-1),\ A(-n),\ A(-n+1),\ A(n-1),\ A(n),\ A(n+1),$

modulo an arbitrary m, all at one time. We call (11) the *signature of* $n \bmod m$. If $m = n$ itself, we are asking in (10) for composites $c = n$ that have signatures

$$-,\ -1,\ -,\ -,\ 0,\ - \pmod n,$$

where we have left four entries blank.

But since we have these numbers anyway let us look at some signatures for $n = m = p =$ prime.

p	Signature $(\bmod p)$						Type
23	1,	−1,	3,	3,	0,	2	S
59	1,	−1,	3,	3,	0,	2	
101	1,	−1,	3,	3,	0,	2	
3	0,	−1,	1,	2,	0,	−1	I
13	0,	−1,	7,	3,	0,	−1	
29	0,	−1,	9,	17,	0,	−1	
5	3,	−1,	2,	2,	0,	0	Q
7	5,	−1,	5,	5,	0,	3	
11	5,	−1,	6,	6,	0,	7	

We prove below that every p is of one of these three types. In the S-type, the signature of p is merely the signature of $n = 1$, *unreduced*, namely:

(12) $\quad A(-2),\ A(-1),\ A(0),\ A(0),\ A(1),\ A(2).$

In the I-type, the signature is

(13) $\quad A(1),\ A(-1),\ p-3-D,\ D,\ A(1),\ A(-1) \qquad (D \not\equiv p-3-D),$

where

(13a) $$D^2 + 3D + 8 \equiv 0 \pmod p.$$

In the Q-type, the signature is

(14) $\quad A,\ A(-1),\ B,\ B,\ A(1),\ C \qquad (B \not\equiv 3),$

where

(14a) $$B^3 - B - 1 \equiv 0 \pmod p,$$

and

(14b) $$A \equiv -B^2 + 3B + 1 \pmod p,$$

and

(14c) $$C \equiv 3B^2 - 2 \pmod p.$$

Note that the parenthetical stipulations on the right of (13) and (14) make the three types disjoint: the S and I are obviously different; Q cannot be S since $B \not\equiv 3 = A(0)$, and Q cannot be I since $B \equiv B$.

So now we strengthen (10) further and demand that the signature of c, like the signatures of all primes, be of one of these three types. Any n that has none of these signatures is certainly composite. For example, the previously mentioned $n = 77$ has

$$25, \quad -1, \quad 46, \quad 30, \quad 29, \quad 4,$$

which not only fails to have $A(77) \equiv 0$, but which also fails in other ways.

2. The Cubic Fields. To strengthen our conditions still further we must identify the Q, I, and S primes. We return to (1) and note that $A(n)$ is the solution of a third-order linear homogeneous difference equation which has the characteristic equation

$$x^3 - x - 1 = 0. \tag{15}$$

This cubic has the discriminant -23 and the three roots

$$\begin{aligned} \alpha &= \ \ 1.324717957, \\ \beta &= -0.6623589786 + 0.5622795121\, i, \\ \gamma &= -0.6623589786 - 0.5622795121\, i. \end{aligned}$$

The theory of difference equations now gives us $A(n)$ explicitly:

$$A(n) = \alpha^n + \beta^n + \gamma^n, \tag{16}$$

and this also holds for $n \leqslant 0$. In all the theory given below, (16) is essential. For n large, (16) gives us the good approximations:

$$\begin{aligned} A(n) &\approx (1.324717957)^n, \\ A(-n) &\approx 2(1.150963925)^n \cos(2.437734932\, n). \end{aligned}$$

We have monotonic growth on the right and slower oscillatory growth on the left where $1.150963925 = \sqrt{\alpha}$.

In the three conjugate cubic fields $Q(\alpha)$, $Q(\beta)$, and $Q(\gamma)$, the rational primes behave in four ways:

The Q primes p have a Jacobi symbol

$$(-23/p) = -1, \tag{17a}$$

and so must lie in these arithmetic progressions:

$$p = 23k + 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, \text{ or } 22. \tag{17b}$$

For any such p, (15) factors as

$$x^3 - x - 1 \equiv (x - a)(x^2 + ax + a^{-1}) \pmod{p}, \tag{18}$$

where the quadratic factor is irreducible (mod p). For example,

$$x^3 - x - 1 \equiv (x - 2)(x^2 + 2x + 3) \pmod{5}.$$

Since a is the only root (mod p) in (18), it follows from (14a) that a, which satisfies

$$a \equiv B \pmod{p}, \tag{19}$$

may be read directly from the signature. It also follows that

$$\left(\frac{a^2 - 4a^{-1}}{p}\right) = \left(\frac{4 - 3B^2}{p}\right) = -1, \tag{20}$$

since the discriminant of the quadratic factor in (18) is a quadratic nonresidue of p. But (20) gives us nothing new since it follows from (18) and (17a).

All primes p *not* in Q have a Jacobi symbol

$$(-23/p) = +1 \text{ or } 0, \tag{21a}$$

and therefore lie in

$$p = 23k + 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, \text{ or } 0. \tag{21b}$$

The I primes p have (15) irreducible. It is known, cf. [4], that these primes have a unique representation

$$8p = u^2 + 23v^2, \qquad u > 0, v \geqslant 0, \tag{22}$$

and they do *not* have a representation

$$p = u^2 + 23v^2, \qquad u \geqslant 0, v > 0. \tag{23}$$

For example,

$$\begin{aligned} 8 \cdot 3 &= 1 + 23, & 3 &\neq u^2 + 23v^2, \\ 8 \cdot 13 &= 9^2 + 23, & 13 &\neq u^2 + 23v^2, \\ 8 \cdot 29 &= 5^2 + 23 \cdot 3^2, & 29 &\neq u^2 + 23v^2. \end{aligned}$$

The I primes cannot have 0 on the right of (21b), and so -23 must have exactly 2 square-roots (mod p). In fact, by (22), they clearly are

$$\sqrt{-23} \equiv \pm \frac{u}{v} \pmod{p}. \tag{24}$$

Now, happily, (13a) gives us

$$(2D + 3)^2 \equiv -23 \pmod{p},$$

so we can read

$$\sqrt{-23} \equiv \pm (2D + 3) \pmod{p} \tag{25}$$

directly from the signature.

Suppose some n has an I signature (13). Then the quadratic form

$$F = \left(n, 2D + 3, \frac{D^2 + 3D + 8}{n}\right) \tag{26}$$

has the discriminant -23. The *quadratic* field $Q(\sqrt{-23})$ has class-number 3 and therefore precisely three reduced quadratic forms of discriminant -23. They are [4]

$$(1, 1, 6), \quad (2, 1, 3), \quad \text{and} \quad (2, -1, 3). \tag{27}$$

These are abbreviations for

$$x^2 + xy + 6y^2, \quad 2x^2 + xy + 3y^2, \quad \text{and} \quad 2x^2 - xy + 3y^2. \tag{28}$$

The form F in (26) must reduce to precisely one of the three forms in (27).

For the sake of any reader not familiar with reduction, we display a not-too-trivial example. Take $n = 92761 =$ prime. Its signature is

$$0, \quad -1, \quad 45335, \quad 47423, \quad 0, \quad -1,$$

an I signature. Then

$$F = (92761, 94849, 24246) \sim (24246, 2135, 47)$$
$$\sim (47, 27, 4) \sim (4, -3, 2) \sim (2, -1, 3).$$

Here, $\sim$ means "is equivalent to", and each transformation

$$(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$$

is obtained by

$$a_2 = c_1, \quad b_2 = -b_1 + 2Nc_1, \quad c_2 = a_1 + \tfrac{1}{2}(b_1 - b_2)N,$$

where the integer N is selected to *minimize* $|b_2|$.

By a simple algorithm [5] based upon the sequence of integers N, the n in (26) has a representation by that form in (28) toward which F reduces. In our example, $x = 178$ and $y = 133$ give

$$92761 = 2 \cdot 178^2 - 178 \cdot 133 + 3 \cdot 133^2.$$

But

$$n = 2x^2 \pm xy + 3y^2 \rightleftarrows 8n = (4x \pm y)^2 + 23y^2,$$

and, if n is odd,

$$n = x^2 + xy + 6y^2 \rightleftarrows n = \left(x + \frac{y}{2}\right)^2 + 23\left(\frac{y}{2}\right)^2$$

since x must be odd, and therefore y must be even. Whereas, if $n = 2$, clearly

$$8 \cdot 2 = 4^2 + 23 \cdot 0^2 \quad \text{and} \quad 2 \neq u^2 + 23v^2.$$

Therefore, if n has an I signature, and if n is prime, the F in (26) must satisfy

$$F \sim (2, \pm 1, 3). \tag{29}$$

The S primes p also satisfy (21a) and (21b), and this time we allow 0 in both equations. The S primes split completely in the cubic fields. Therefore

$$x^3 - x - 1 \equiv (x - a)(x - b)(x - c) \pmod{p} \tag{30}$$

also splits completely. The S primes now have a unique representation (23) and they do *not* have a representation (22). For example,

$$59 = 6^2 + 23, \quad 472 \neq u^2 + 23v^2.$$

Clearly, (24) remains valid, but we now have no counterpart to (25) since the uninformative S signature tells us nothing.

We are counting $p = 23$, the unique ramified prime, as an S prime since it has an S signature. Its special role is seen in

$$x^3 - x - 1 \equiv (x - 3)(x - 10)^2 \pmod{23},$$

with its double root, unlike the three distinct roots in (30), and also in its degenerate representation: $23 = 23$.

To round out the foregoing we note that Q primes cannot have either representation, (22) or (23), since both imply (24).

We should also note that while a prime can have at most one representation by either (22) or (23), but not by both, a composite may have many representations, and

may have both, thus

$$377 = 13 \cdot 29 = 3^2 + 23 \cdot 4^2 = \frac{1}{8}(53^2 + 23 \cdot 3^2).$$

But here 13 and 29 are both I primes. We will need later the fact that a product of any number of S primes can only have the representations in (23). That is because the three forms in (28) constitute a group under composition for which $x^2 + xy + 6y^2$ is the identity. A product of identities is the identity. Therefore if n is a product of S primes only, and if it has an I signature, then (29) *must fail*. Somewhat similarly, if n is a product of S primes only, and if it has a Q signature, then (17a) *must fail*.

A fourth distinction among the S, I, and Q primes concerns the *period* of $A(n)$ (mod p). This sequence is always periodic, but the period divides

$$p - 1, \quad p^2 + p + 1, \quad \text{or} \quad p^2 - 1 \tag{31}$$

according as p is in S or I or Q, respectively. The proof is again given later but we do note, at once, that if the period divides $p - 1$, then the signature of p (mod p) is clearly the signature of $n = 1$ unreduced; i.e., we have an S signature.

It follows that if the period of a Q prime p divided $(p - 1)$, and not merely $(p + 1)(p - 1)$, that that p would have an S signature. But that cannot be since $B \not\equiv 3$ in (14). If $B = 3$ in (14a), then $p \mid 23$, which is impossible. It follows that *some* proper factor in $(p + 1)$ must remain in the period.

By Chebotarev's theorem, the S, I, and Q primes occur in the proportions

$$\frac{1}{6} : \frac{1}{3} : \frac{1}{2}, \tag{32}$$

asymptotically speaking. That is so because the Galois group of (15) is S_3, the symmetric group on three letters.

Definition. We now say that n has an *acceptable signature* (mod n) if

(A) It has a Q signature with (14) and (14a, b, c), and if (17a) also holds with n written in place of p; or if

(B) It has an I signature with (13) and (13a), and if (21a) holds without the 0, and if (29) also holds. Again, replace p with n; or if

(C) It has an S signature (12), and (21a) holds with $p = n$, allowing the 0.

Commentary. It can be questioned whether the inclusion of (14a), (14b) and (14c) in (A) is redundant. But (14a, b, c) are very cheap, arithmetically speaking, and so we include them in the definition. A stronger objection may be raised to the inclusion of (29) in (B). It is also fast but not as trivial as, say, (13a). An investigation in Section 8 below suggests that there *may be* I-type composites in Perrin's sequence if we omit (29). To be safer, we are therefore including it. In contrast, our demands upon S signatures above are much weaker. That is because (12) is uninformative; it tells us nothing about (24) or (30). This will require our attention and we will return to the question in Sections 9, 10, and 11.

3. Two Similar Sequences. The smallest negative discriminant for a cubic field is the -23 above. The next two are -31 and -44. The discriminant of

$$x^3 - x^2 - 1 = 0 \tag{33}$$

is -31 and (33) gives us

$$A(1) = 1, \quad A(2) = 1, \quad A(3) = 4, \quad A(n+3) = A(n+2) + A(n). \tag{34}$$

This recurrence also reverses:

$$A(0) = 3, \quad A(-1) = 0, \quad A(-2) = -2, \ldots.$$

Congruences (4) and (5) remain valid, and we now have

$$p \mid A(-p) \quad \text{and} \quad p \mid A(p) - 1. \tag{35}$$

Congruences (9) remain valid and since

$$A(-11) = A(-1),$$

again, we find that

$$121 \mid A(-121),$$

but, again, 121 fails on the right:

$$121 \nmid A(121) - 1.$$

This time,

$$4 \mid A(4) - 1 \quad \text{and} \quad 4 \nmid A(-4).$$

This $A(n)$ has a very similar $O(\log n)$ algorithm and again we have the three types of signatures, still given by (12), (13), and (14), but with $A(n)$ having its new meaning. But here are changes:

For I primes,

$$D^2 + 3D + 10 \equiv 0 \pmod{p}. \tag{36}$$

For Q primes,

$$B^3 + B + 1 \equiv 0 \pmod{p}, \tag{37a}$$

$$A \equiv 3B^2 + 2 \pmod{p}, \tag{37b}$$

$$C \equiv B^2 - 3B + 1 \pmod{p}. \tag{37c}$$

This time (16) holds for

$$\begin{aligned} \alpha &= \ \ 1.465571232, \\ \beta &= -0.232785616 + 0.7925519925\, i, \\ \gamma &= -0.232785616 - 0.7925519925\, i, \end{aligned}$$

and so now $A(n)$ grows faster but rotates a little slower for $n < 0$.

The three types of primes are as before with 23 replaced consistently by 31, e.g., Q primes have

$$(-31/p) = -1,$$

I primes have a unique representation

$$8p = u^2 + 31v^2,$$

and S primes split completely:

$$x^3 - x^2 - 1 \equiv (x-a)(x-b)(x-c) \pmod{p}. \tag{38}$$

This time 31 is the sole ramified prime. The proportions of the three types of primes and their periods are as before.

Of course, the assignment of any prime to S, I, or Q will generally not be the same as it was before. Particular interest will attach to the $1/36$ of the primes that are S in both cubic fields. There are only three such $p < 1000$. They are

$$\begin{aligned} 173 &= 9^2 + 23 \cdot 2^2 = 7^2 + 31 \cdot 2^2, \\ 607 &= 20^2 + 23 \cdot 3^2 = 24^2 + 31, \\ 853 &= 5^2 + 23 \cdot 6^2 = 27^2 + 31 \cdot 2^2. \end{aligned}$$

The relative scarcity of such p will have importance later.

From (33) and (37a) it is clear that the realtionship between B and a for Q primes is not what it was in (19). We now reach ahead to the theory section and quote some of the general results proved there. They will enable us to deduce such relationships as in (36) and (37a, b, c) from a general theory.

In this theory we have the cubic

$$x^3 - A(1)x^2 + A(-1)x - 1 = 0, \quad A(0) = 3, \tag{39}$$

and the sequence

$$A(n+3) = A(1) \cdot A(n+2) - A(-1) \cdot A(n+1) + A(n). \tag{40}$$

Congruences (4), (5), (9) remain valid. So does (16). We are primarily interested in those cubics where (39) is irreducible and has the S_3 group, as we do have in the -23 and -31 examples. There are then the same three types of primes except that the ramified primes may act differently in the general case.

The S and Q primes have the same signatures (12) and (14), but the congruences for B, A, and C in (14) are specific to the particular sequence (40). For a Q prime p, (18) generalizes to

$$\begin{aligned} 0 &\equiv x^3 - A(1)x^2 + A(-1)x - 1 \\ &\equiv (x-a)\left(x^2 + (a - A(1))x + a^{-1}\right) \pmod{p}, \end{aligned} \tag{41}$$

and from its unique root $a \pmod p$ we obtain the important relationships:

$$B \equiv \left[A(1)^2 - A(-1)\right]a - A(1)a^2 \pmod{p}, \tag{42a}$$

$$A \equiv a^{-2} + 2a \pmod{p}, \tag{42b}$$

$$C \equiv a^2 + 2a^{-1} \pmod{p}. \tag{42c}$$

It is only in Perrin's sequence ($A(1) = 0$, $A(-1) = -1$) that (42a) gives $B \equiv a \pmod p$.

In the theory, it is natural to give a the central role, and that gives us (42a, b, c). Whereas, operationally speaking, we obtain the signature (14), and B not only has the central position, literally speaking, but it is also preferable to give it the central role, computationally speaking. We therefore invert (42a) by squaring it and reducing the resulting quartic in a by the use of

$$a^3 - A(1)a^2 + A(-1)a - 1 \equiv 0 \pmod{p}. \tag{43}$$

That gives us a as a function of B instead. For our present -31 case that function is

$$a \equiv B^2 + 1 \pmod{p}. \tag{44}$$

With a as a function of B we now obtain the cubic satisfied by B. This is (37a) in the present case. We then obtain A and C as functions of B from (42b, c). These were (14b, c) in Perrin and (37b, c) in the present case.

In contrast to the universal Q signature (14), the general I signature does not always remain (13). If the discriminant of (39) is d, the I signature is

$$A(1),\quad A(-1),\quad D',\quad D,\quad A(1),\quad A(-1), \tag{45}$$

where

$$D' + D \equiv A(1)A(-1) - 3, \tag{46}$$

and

$$\pm (D - D') \equiv \sqrt{d}\,. \tag{47}$$

Note that -31 and -23 both have (13) since they both have $A(1)A(-1) = 0$. Note that (13a) and (36) are both obtained by squaring (47) and that they are valid for the I prime $p = 2$. Note that we can now drop the parenthetical ($D \not\equiv D'$) since $d \equiv 0 \pmod{p}$ only for the ramified primes. Finally, we stress the point that d is the discriminant of the cubic *polynomial* and not necessarily that of the cubic *field*. In -23, -31, and -44 these two discriminants are equal, but that is not always the case in (39).

Now we return to the -31 sequence (34) and quickly complete its treatment. The arithmetic progressions for Q, I, and S primes are obvious. The quadratic field $Q(\sqrt{-31}$ again has class number 3, and there are three reduced forms:

$$(1,1,8),\quad (2,1,4),\quad \text{and}\quad (2,-1,4). \tag{48}$$

For I primes, the relation equivalent to the previous (29) is now

$$F = \left(n, 2D + 3, \frac{D^2 + 3D + 10}{n}\right) \sim (2, \pm 1, 4). \tag{49}$$

The definitions of acceptable signatures for (34) is now clear.

In the -44 sequence, some things are familiar and some things are new. We have

$$x^3 - x^2 - x - 1 = 0, \tag{50}$$

$$A(1) = 1,\quad A(2) = 3,\quad A(3) = 7,$$
$$A(n+3) = A(n+2) + A(n+1) + A(n), \tag{51}$$
$$A(0) = 3,\quad A(-1) = A(-2) = -1.$$

We now have

$$p \mid A(-p) + 1,\quad p \mid A(p) - 1, \tag{52}$$

and behavior like this:

$$A(-5) = A(-1) = -1,\quad 25 \mid A(-25) + 1,\quad 25 \nmid A(25) - 1,$$

looks familiar.

But now 2 and 11 both ramify and some things are new. From (51), *all* $A(n)$ are odd. We have

$$2p \mid A(-2p) + 1 \tag{53}$$

for *every* p, including $p = 2$, but we also have

$$2p \mid A(2p) - 3, \tag{54}$$

and therefore $2p$ always fails on the right since

$$2p \nmid A(2p) - 1.$$

Let us prove (53), (54) at once by using a *Doubling Rule* that lies at heart of the $O(\log n)$ algorithm.

Doubling Rule. For all $A(n)$ above, and all n, we have

$$A(2n) = (A(n))^2 - 2A(-n), \quad A(-2n) = (A(-n))^2 - 2A(n). \tag{55}$$

Proof.

$$(A(n))^2 = (\alpha^n + \beta^n + \gamma^n)^2 = \alpha^{2n} + \beta^{2n} + \gamma^{2n} + 2(\beta^n\gamma^n + \alpha^n\gamma^n + \alpha^n\beta^n).$$

But the last term equals $2A(-n)$ since $\alpha\beta\gamma = 1$ for all of our $A(n)$. Therefore,

$$A(2n) = (A(n))^2 - 2A(-n),$$

and replacing α, β, and γ by their reciprocals gives us the second equation in (55). □

Therefore, (52) gives

$$A(2p) \equiv 1^2 - 2(-1) = 3 \pmod p,$$
$$A(-2p) \equiv -1^2 - 2 \cdot 1 = -1 \pmod p.$$

Since $A(n) \equiv 1 \pmod 2$ for all n, (53) and (54) follows. □

Q signatures now satisfy

$$B^3 + B^2 + 3B - 1 \equiv 0, \tag{56a}$$

$$A \equiv B^2 + 3B + 3, \tag{56b}$$

$$C \equiv 2B^2 + B + 4, \tag{56c}$$

and give us

$$a \equiv \tfrac{1}{2}(B^2 + 2B + 3), \quad B \equiv 2a - a^2. \tag{57}$$

They are acceptable if

$$(-11/n) = -1. \tag{58}$$

I signatures now are

$$A(1), \quad A(-1), \quad n - 4 - D, \quad D, \quad A(1), \quad A(-1), \tag{59}$$

(with 4 instead of 3), and where

$$D^2 + 4D + 15 \equiv 0 \pmod n. \tag{60}$$

Also new is the unique representation

$$3p = u^2 + 11v^2, \qquad u > 0, v > 0, \tag{61}$$

for I primes.

This time, -44 is not a fundamental discriminant as -23 and -31 were. The corresponding quadratic field $Q(\sqrt{-11})$ has discriminant -11, not -44. It has class number 1 and only one reduced form: $(1, 1, 3)$. But the *order* in this field of

discriminant −44 does have class number 3 and the forms

$$(1,0,11),\quad (3,2,4),\quad (3,-2,4). \tag{62}$$

Acceptable I signatures must have

$$(-11/n) = +1 \tag{63}$$

and

$$F = \left(n, 2D+4, \frac{D^2+4D+15}{n}\right) \sim (3, \pm 2, 4). \tag{64}$$

S primes have the unique representation

$$p = u^2 + 11v^2, \qquad u \geqslant 0, v > 0, \tag{65}$$

and acceptable S signatures have

$$(-11/n) = +1 \quad \text{or} \quad 0. \tag{66}$$

The ramified $p = 11$ is an S prime, but $p = 2$ simply does not fit this classification. The Kronecker symbol $(-11/2) = -1$, and obviously neither 2 nor 6 equals $u^2 + 11v^2$. In those ways, 2 looks like a Q prime. On the other hand, the cubic splits completely (mod 2), the period equals $1 = 2 - 1$, and its signature is S (in a trivial way). In those ways, 2 looks like an S prime. The ambiguity comes from the two discriminants, −44 and −11. In $Q(\sqrt{-11})$, 2 does not ramify; it is inert instead. We already saw unusual behavior in the composites $2p$, and we may anticipate other such anomalies with even composites. In fact, (56b, c) assumed that the modulus was odd.

For reference, we record S primes < 1000 common to −23 and −44:

$$\begin{aligned} 599 &= 24^2 + 23 \quad\;\; = 18^2 + 11 \cdot 5^2, \\ 883 &= 26^2 + 23 \cdot 3^2 = 28^2 + 11 \cdot 3^2, \\ 991 &= 28^2 + 23 \cdot 3^2 = 10^2 + 11 \cdot 9^2, \end{aligned}$$

and common to −31 and −44:

$$\begin{aligned} 47 &= 4^2 + 31 \quad\;\; = 6^2 + 11, \\ 617 &= 11^2 + 31 \cdot 4^2 = 21^2 + 11 \cdot 4^2. \end{aligned}$$

There is no S prime < 1000 common to all three fields. That is not surprising since $\pi(1000) = 168 < 216 = 6^3$.

As an exercise, we compute the real root α of (50) with the Doubling Rule. Starting with $A(-1) = -1$, $A(1) = 1$, we double the arguments five times and obtain $A(32) = 294294531$. Since this is very close to α^{32}, we have $\alpha = 1.839286755$.

4. Reasons Why Composites with Acceptable Signatures Must be Rare. With the foregoing as background, we now give four reasons to believe that such composites are rare, leaving it open, in this section, whether they do exist. Let us first contrast our third-order $A(n)$ with the classic second-order $V(n)$ of Lucas. Here,

$$V(1) = 1, \quad V(2) = 3, \quad V(n+2) = V(n+1) + V(n), \tag{67}$$

and we have

$$n \mid V(n) - V(1) \tag{68}$$

for all primes n and for some composites.

There are two kinds of primes for (67) besides the ramified $p = 5$. The S primes p have $(5/p) = +1$, $x^2 - x - 1 \equiv 0$ splits (mod p), and the period of $V(n)$ (mod p) divides $p - 1$. The I primes p have $(5/p) = -1$, $x^2 - x - 1 \equiv 0$ is irreducible (mod p), and the period divides $2(p + 1)$. Each type comprises one-half of all primes.

Thus, in $V(n)$, *all* primes have periods bounded linearly: by $p - 1$ or by $2(p + 1)$, whereas, in $A(n)$, $5/6$ of the primes have periods bounded quadratically: by $p^2 + p + 1$ or by $p^2 - 1$. Further, the actual periods in $A(n)$ are odd at least $1/3$ of the time and are not infrequently themselves prime. Thus, in Perrin's $A(n)$, $p = 2$ has the period 7 and $p = 3$ has the period 13. In $V(n)$, the periods are usually even, usually much smaller, and seldom are they prime. Without arguing it more fully, this makes it harder to find composites satisfying

$$c \mid A(c) - A(1),$$

even taken alone, than it is to find composite solutions of (68).

Aside from the larger period bounds in $A(n)$ for most of the primes, it also occurs less often that the S and I primes have periods that are smaller than these bounds. In $V(n)$, $1/2$ of the S primes have periods dividing $(p - 1)/2$. Whereas, in Perrin, the S primes have periods dividing $(p - 1)/2$ if, and only if, we have

$$(a/p) = (b/p) = (c/p) = 1 \tag{69}$$

in (30). Since $abc \equiv 1$, it suffices that $(a/p) = (b/p) = 1$. This should occur for $1/4$ of the S primes, not $1/2$. In Appendix 1, we list the periods of the first 120 p in Perrin; in fact, among the 16 S primes there, four have periods of $(p - 1)/2$. The Q primes frequently have periods $< p^2 - 1$ since $(p - 1)(p + 1)$ is always divisible by 24, and is divisible by 5 for $2/5$ of the p, etc.

The second reason for the rarity of acceptable composites is the fact that the density of the S primes is only $1/6$. That will become very clear as we proceed and shows the value in using cubic polynomials having the S_3 group.

Our third and fourth reasons are very strong since they sieve out large classes of composites c divisible by a prime p by merely stipulating

$$A(-c) \not\equiv A(-1) \quad \textit{or} \quad A(c) \not\equiv A(1) \pmod{p}, \tag{70}$$

without demanding the much stronger (mod c) condition, let alone the even stronger acceptable signature condition.

We use

$$A(mp) \equiv A(m) \pmod{p}, \tag{71}$$

which we prove later, and from which (4) and (5) follow immediately. We want all composites

$$c = mp$$

that satisfy the relatively weak (70).

Let p be fixed. By (71), (70) becomes

$$A(-m) \not\equiv A(-1) \quad \textit{or} \quad A(m) \not\equiv A(1) \pmod{p}. \tag{72}$$

Now

$$A(p^k) \equiv A(1), \quad A(-p^k) \equiv A(-1) \pmod{p} \tag{73}$$

for all $k = 0, 1, 2, \ldots$ by induction using (71). Let $W = W(p)$ be the period of $A(n)$ (mod p). It equals $p - 1$, $p^2 + p + 1$ or $p^2 - 1$, or some divisor thereof, according as p is S, I, or Q, respectively. In any case, W is prime to p. After we go through W multiples of p:

$$p, \quad 2p, \quad 3p, \ldots, Wp,$$

$A(mp)$ will repeat (mod p). Therefore, for every m such that

$$mp = kWp + p^n, \qquad k = 0, 1, \ldots, \qquad n = 1, 2, \ldots, \tag{74}$$

we do have

$$A(-mp) \equiv A(-1), \quad A(mp) \equiv A(1) \pmod{p} \tag{75}$$

and $c = mp$ *does not* satisfy (70).

In (74), we can restrict n to those values where $n \leqslant 1$, 2, or 3 for S primes, Q primes, or I primes, respectively, since, for all larger powers p^r, one can show that these powers already lie in the arithmetic progressions

$$mp = kWp + p^n, \qquad k = 0, 1, \ldots, \tag{76}$$

where n is so restricted.

We prove below that *all m other* than those given by (76) satisfy (72) if p is an I or Q prime. Therefore, all such composites mp must certainly fail to have acceptable signatures. Let us see the effect of that in Perrin's $A(n)$. We have

$$W(2) = 7, \quad W(3) = 13, \quad W(5) = 24, \quad W(7) = 48.$$

Therefore, (75) holds for, and only for, those multiples of p given by

$$\begin{aligned} c &= 14k + 2, 4, 8 \quad (\text{for } p = 2), \\ c &= 39k + 3, 9, 27 \quad (\text{for } p = 3), \\ c &= 120k + 5, 25 \quad (\text{for } p = 5), \\ c &= 336k + 7, 49 \quad (\text{for } p = 7). \end{aligned} \tag{77}$$

All other multiples of p, namely:

$$\begin{aligned} &c = 14k, 14k + 6, 14k + 10, 14k + 12, \\ &c = 39k, 39k + 6, 39k + 12, 39k + 15, \ldots, 39k + 36, \end{aligned}$$

etc., must certainly fail (10) since they already fail the weaker (75). With $p = 2$, we therefore delete $2/7$ of all composites; with $p = 3$, we delete $10/39$ of those remaining, etc. This sieving leaves only relatively few composites. Of course, the -31 and -44 $A(n)$ behave in similar ways.

A practical remark concerning the sieving: Since the arithmetic progressions to be deleted are much more numerous than those in (77) which are to be kept, it is clearly quicker to delete *all* multiples of p and then to put those in (77) back in.

Sieving with the S primes is a delicate matter. For example, take $p = 59$ or 101 in Perrin. Then, the *same restrictions* hold: we must have

$$m \cdot 59 = k \cdot 58 \cdot 59 + 59, \quad \text{or} \quad m \cdot 101 = k \cdot 100 \cdot 101 + 101,$$

or else (75) fails. In fact, in all three $A(n)$ examined above, namely, those for -23, -31, and -44, *we do not know* of a *single* S prime where the restrictions in (76) do not hold. Nonetheless, it is not proved that (76) holds for all S primes in all three of these $A(n)$.

In the general theory (39), it is not difficult to construct S primes that are not restricted by (76). For example,

$$x^3 - 7x^2 + 21x - 1 = 0$$

has $p = 29$ as an S prime that has the period $W = 7$. Then take $m = 9$. Clearly,

$$9 \cdot 29 \neq k \cdot 7 \cdot 29 + 29,$$

and yet, with $m = 9$, (75) is true. We designate such an m, that lies outside of the progressions (76), but for which (75) is true, as an *outsider*. We will see the importance of this concept later.

For the present, the possible existence of such outsiders therefore makes it improper to sieve with S primes unless they have been examined numerically, like 59 and 101 above, and found to be free of outsiders.

Our fourth reason for the scarcity of acceptable composites is much simpler; it has no such subtle complications. Return to (72) and now keep m fixed and let p vary. Then *any* p with mp acceptable must obviously divide the

(78) $$\text{G.C.D. of } A(-m) - A(-1) \quad \text{and} \quad A(m) - A(1).$$

Consider Perrin's $A(n)$ and $m = 2$. The GCD equals 2 and p could only be 2 itself. Likewise, for $m = 3, 5, 7, 13, 19$, and 31, the GCD equals m itself and $c = m^2$ is the only possible acceptable composite. But we already saw in Section 1 that $c = p^2$ is not acceptable for all $p \leqslant 521$. For other $m \leqslant 40$, we find the following: For some m such as 6, 10, 12, 20, etc., the GCD equals 1 and no $c = mp$ even exist. For m such as 11, 23, etc., the GCD equals $2m$ and both possibilities, $c = m^2$ and $c = 2m$, have already been eliminated. For m such as 14, which has GCD = 3, the only $c = 14 \cdot 3 = 6 \cdot 7$ has already been deleted by the smaller $m = 6$.

The only $m \leqslant 40$ that require a new idea are the prime powers: $m = q^n$. Here, q divides the GCD, and we may eliminate $c = q^{n+1}$ recursively by a generalization of (9) that we prove later. That is

$$A(p^{n+1}) \equiv A(p^n) \pmod{p^{n+1}}, \qquad A(-p^{n+1}) \equiv A(-p^n) \pmod{p^{n+1}}.$$

Actually, all the GCD for $m \leqslant 40$ have few prime divisors, and one easily shows that *no* $c = mp$ can be acceptable for these m. One could easily go beyond $m = 40$ by programming (78). If there is *any* composite with an acceptable signature, and there is, this progression of impossible m must be interrupted.

5. The Algorithm. Two of the acceptable composites for Perrin's $A(n)$ that were just alluded to are

$$C = 7045248121 \quad \text{and} \quad 7279379941.$$

They have acceptable S-signatures and are discussed in detail in the next section. But since they, and other acceptable composites that we have for the -23, -31 and -44 $A(n)$, have at least eight decimal digits, let us return to our construction of the $O(\log n)$ algorithm. The direct $O(n)$ computation by (1), (34), or (51) would surely be wasteful and tedious.

Suppose we want the signature of $N \pmod m$ and already have that of $n \pmod m$ for a certain $n < N$. We have the sextet in (11) (mod m). We use the Doubling Rule and compute those $A(j)$ having doubled arguments, namely,

(79) $$A(-2n-2), \quad A(-2n), \quad A(-2n+2), \quad A(2n-2), \quad A(2n), \quad A(2n+2),$$

all (mod m). If $A(j)$ is the Perrin sequence, we can fill in the gaps in (79) as follows: First,

$$A(-2n-1) \equiv A(-2n+2) - A(-2n), \quad A(2n-1) \equiv A(2n+2) - A(2n).$$

Then,

$$A(-2n+1) \equiv A(-2n-1) + A(-2n-2),$$
$$A(2n+1) \equiv A(2n-1) + A(2n-2).$$

Now we have five successive values centered around $A(-2n)$ and $A(2n)$, and, *ipso facto*, we have the signatures of $2n$ and $2n+1$ (mod m).

Now write N in binary and read it from left to right one bit at a time. The first bit reads 1. The first two equal 2(1) or 2(1) + 1. The first k equal some number n, and the first $k+1$ equals $2n$ or $2n+1$ according as the $(k+1)$st bit equals 0 or 1. Therefore, in $O(\log N)$ operations we have the signature of N (mod m) starting with the known signature for $n = 1$.

The algorithms for -31 and -44 are only slightly different and are left as an exercise. The reader who knows a little programming can now write a program for his own machine. For those who know Hewlett-Packard programming, see Appendix 2.

It is clear that the main computation time, when N is large, is used in computing the squares $A(n)^2$ for the Doubling Rule. That is also true in most of the classical primality tests, and much of this time can be saved by using Toom-Cook arithmetic [6].

6. The Carmichael Solutions. The composites listed at the beginning of the last section are

$$C_1 = 7045248121 = 821 \cdot 1231 \cdot 6971,$$

where

$$821 = 27^2 + 23 \cdot 2^2, \quad 1231 = 32^2 + 23 \cdot 3^2, \quad 6971 = 18^2 + 23 \cdot 17^2,$$

and

$$C_2 = 7279379941 = 211 \cdot 3571 \cdot 9661,$$

where

$$211 = 2^2 + 23 \cdot 3^2, \quad 3571 = 58^2 + 23 \cdot 3^2 \quad \text{and} \quad 9661 = 47^2 + 23 \cdot 18^2.$$

Carmichael numbers

$$C = p_1 \cdot p_2 \cdot p_3 \cdots \tag{80}$$

are square-free products of three or more primes p_i such that

$$p_i - 1 \mid C - 1 \tag{81}$$

for each i. It follows that

$$C \mid a^C - a \tag{82}$$

for every integer a.

C_1 and C_2 are Carmichaels whose factors are S primes for Perrin's $A(n)$. Since the period of $A(n)$ (mod p_i) divides $p_i - 1$ it also divides $C - 1$. Therefore the signature

of $C \pmod{p_i}$ is

$$1, \quad -1, \quad 3, \quad 3, \quad 0, \quad 2 \tag{83}$$

for each i. Therefore the signature of $C \pmod{C}$ is also that in (83). They are acceptable since both have S signatures and $C \equiv 16$ or $1 \pmod{23}$.

Wagstaff [7] computed all 2163 Carmichaels $< 25 \cdot 10^9$. Among all of these only C_1 and C_2 are products of S primes for the -23 sequence exclusively.

For the -31 sequence, we have three such Carmichaels:

$$C_3 = 6693621481 = 607 \cdot 1213 \cdot 9091,$$
$$C_4 = 8904870001 = 31 \cdot 173 \cdot 521 \cdot 3187, \quad \text{and}$$
$$C_5 = 22008493921 = 431 \cdot 1721 \cdot 29671.$$

Note that C_4 contains the ramified S prime 31. An interested reader can easily supply the quadratic partitions

$$p_i = u^2 + 31v^2.$$

For example, $521 = 5^2 + 31 \cdot 4^2$, a sum of a square and a perfect number.

In the -44 sequence, one finds that there are more, relatively small, S primes than occur in either of the -23 or the -31 sequences, and therefore one expects more Carmichael solutions $< 25 \cdot 10^9$. Actually, there is only one:

$$C_6 = 1833328621 = 103 \cdot 3877 \cdot 4591$$

where

$$103 = 2^2 + 11 \cdot 3^2, \quad 3877 = 59^2 + 11 \cdot 6^2, \quad \text{and} \quad 4591 = 46^2 + 11 \cdot 15^2.$$

As Casey Stengel used to say, "You could look it up!"

It is interesting to verify how all of the C_i above elude the sieving in Section 4 that gave us the "3rd and 4th reasons" there. For example, compare

$$C_1 = 10465 \cdot 820 \cdot 821 + 821 = 4653 \cdot 1230 \cdot 1231 + 1231$$
$$= 145 \cdot 6970 \cdot 6971 + 6971$$

with (76) for the third reason. Thus, C_1 has nothing to do with the outsiders introduced there. Actually, we prove below that if p is an S prime and mp has an S signature $(\text{mod } p)$, then m cannot be an outsider of p. Therefore, without calculation, we know that the same thing happens in all of our C_i.

Again, in C_2, take $m = 211 \cdot 3571 = 753481$. Since

$$m \cdot 9661 = 78 \cdot 9660 \cdot 9661 + 9661,$$

we must have

$$A(-m) \equiv A(-1) \quad \text{and} \quad A(m) \equiv A(1) \pmod{9661}.$$

Therefore, $C_2 = m \cdot 9661$ is *not* deleted by m "for the fourth reason", and, since it is not deleted at all, the "progression of impossible m" that is referred to at the end of Section 4 must certainly "be interrupted" at $m = 753481$ if not sooner.

None of these six C_i has an acceptable signature in either of the other two $A(n)$. For example, consider C_3 in Perrin. Since $A(607 \cdot 1213) \equiv 9051 \not\equiv 0 \pmod{9091}$, it must fail for this fourth reason condition. Similarly, C_1 fails in the -31 sequence since $A(821 \cdot 1231) \equiv 4749 \pmod{6971}$ for that sequence.

Of course, a C_i would be acceptable in another $A(n)$ if all of its prime factors were also S primes in that $A(n)$. But that does not happen in these six C_i. Consider $p = 29671$ in C_5. We have

$$p = 68^2 + 23 \cdot 33^2 = 60^2 + 31 \cdot 29^2 = 86^2 + 11 \cdot 45^2,$$

so p is S in all three fields. Further, since

$$C_5 = 25 \cdot 29670 \cdot 29671 + 29671,$$

we must have

$$A(-C_5) \equiv A(-1), \quad A(C_5) \equiv A(1) \pmod{29671} \tag{84}$$

in *all three* sequences. Nonetheless, C_5 does not have an S signature in either the -23 or the -44 sequence. The other two factors in C_5 are 431 and 1721. They are both Q in Perrin and are Q and I, respectively, in -44. As we indicated above, there is no $p < 1000$ that is S in all three fields, and one notes that each of the six C_i has at least one prime factor < 1000.

Another point worth recording: Take $m = 431 \cdot 1721 = 741751$, which is a little smaller than the $m = 753481$ examined for C_2. By (84), C_5 would *not* be sieved out by this smaller m for Perrin's sequence. However, the Q prime 431 has a period $W = (431^2 - 1)/2$ in Perrin. Since

$$C_5 = 549 \cdot W \cdot 431 + 72671 \cdot 431,$$

and 72671 is neither 1 nor 431, C_5 would have already been sieved out by 431 for the third reason.

We will return to Carmichael solutions later.

7. The O_i and the T_i. J. Owings suggested the following possibility. Let p and $2p - 1$ both be S primes, and suppose, as in Section 4, that

$$W(2p - 1) \mid p - 1. \tag{85}$$

We argued heuristically in Section 4 that (85) has a probability of $1/4$. If (85) does hold, then

$$N = p(2p - 1) \tag{86}$$

has an acceptable S signature since $N = (2p + 1)(p - 1) + 1$. We systematically searched for such $N < 10^9$ for Perrin's $A(n)$. One can restrict the search to p satisfying

$$p \equiv 1, \quad 13, \quad 25, \quad 39 \quad \text{or} \quad 41 \pmod{46}$$

since only such p have $(p/23) = (2p - 1/23) = +1$.

There are only three such $N < 10^9$ where p and $2p - 1$ are both S primes. In the first,

$$N = 4567 \cdot 9133,$$

N fails since $W(9133) \nmid 4566$. But

$$O_1 = 4831 \cdot 9661 = 46672291 \tag{87}$$

is acceptable, and it is much smaller than our C_i. Note that the factor 9661 also occurs in C_2, and that, in this O_1, $m = 4831$ already interrupts the "progression of impossible m."

The third N occurred just before our 10^9 limit and is also acceptable. It is

$$O_2 = 22027 \cdot 44053 = 970355431. \tag{88}$$

The eight acceptable composites so far displayed, the six C_i and the two O_i, are insufficient to settle a question that arises in Section 9 below. We therefore decided to compute more O_i since that is quite easy to do.

In the -31 sequence, there are eight candidates $N < 5 \cdot 10^9$ starting with $N = 607 \cdot 1213$. But they all fail; we have no O_i for this sequence.

In the -44 sequence, there are 14 candidates $N < 5 \cdot 10^9$ starting with $N = 199 \cdot 397$. Three succeed:

$$\begin{aligned} O_3 &= 16087 \cdot 32173 = 517567051, \\ O_4 &= 24379 \cdot 48757 = 1188646903, \\ O_5 &= 32077 \cdot 64153 = 2057835781. \end{aligned} \tag{89}$$

We then returned to -23. There are 25 additional candidates $N < 25 \cdot 10^9$. Five succeed:

$$\begin{aligned} O_6 &= 40459 \cdot 80917 = 3273820903, \\ O_7 &= 50647 \cdot 101293 = 5130186571, \\ O_8 &= 51199 \cdot 102397 = 5242624003, \\ O_9 &= 85837 \cdot 171673 = 14735895301, \\ O_{10} &= 102259 \cdot 204517 = 20913703903. \end{aligned} \tag{90}$$

We will return to the O_i later.

An obvious generalization of (86) is

$$N = p(kp - k + 1)$$

for $k = 3, 4, \ldots$. We examined only

$$N = p(3p - 2), \tag{91}$$

where we need

$$W(3p - 2) \mid p - 1. \tag{92}$$

If (92) holds, (91) is acceptable with an S signature, and we call it T_i.

We expect the number of T_i to be somewhat less than the number of O_i up to some large limit M. Specifically, we expect

$$\frac{\text{number of } T_i}{\text{number of } O_i} \to \frac{8}{9}\sqrt{\frac{2}{3}} = 0.726 \tag{93}$$

as $M \to \infty$. Here is the argument: the probability of (92) is now $1/9$ instead of $1/4$. But $3 \mid p(2p - 1)$ for $2/3$ of the trials as p runs through the integers while $3 \mid p(3p - 2)$ for only $1/3$ of the trials since $3 \nmid 3p - 2$. Finally, p in (86) $\sim \sqrt{N/2}$ while p in (91) $\sim \sqrt{N/3}$ as $M \to \infty$. Putting the three variables together gives the right side of (93).

The statistics in Perrin do not agree with this at all if we go to only 10^9. There are no less than 14 candidates (91) $< 10^9$, beginning with $N = 883 \cdot 2647$. Of these, five are acceptable:

$$\begin{aligned} T_1 &= 3037 \cdot 9109 = 27664033, \\ T_2 &= 5851 \cdot 17551 = 102690901, \\ T_3 &= 6607 \cdot 19819 = 130944133, \\ T_4 &= 13487 \cdot 40459 = 545670533, \\ T_5 &= 16883 \cdot 50647 = 855073301. \end{aligned}$$

Note that T_1 is our smallest acceptable so far and it also gives us a new $m = 3037$.

With a limit of 10^9, the v in $p = u^2 + 23v^2$ has hardly gone through one complete set of residues (mod 23), and it is not surprising that (93) is so wrong at this limit. Cubic fields have a number of famous problems where the early distribution is quite different than the asymptotic distribution, e.g., cf. [8] for Kummer's conjecture or [9] for the density of cubic fields. Note that the O_i in Perrin began with 2 successes out of 3 candidates but ended with 7 out of 28, just as predicted.

We will return to the T_i also.

8. Questions. (A) Are there infinitely many acceptable composites for each of our $A(n)$? Almost certainly, yes, but we cannot prove it. Almost certainly, there are infinitely many Carmichael solutions, and yet it has never been proved that there are infinitely many Carmichael numbers.

On a large computer, one could create Carmichael solutions almost at will, as follows: Suppose p, $2p - 1$, and $3p - 2$ are all prime. Therefore, p must be $6m + 1$. It cannot be $6m - 1$ since that implies that $2p - 1 = 12m - 3$ is not prime. Consider their product

$$n = (6m + 1)(12m + 1)(18m + 1). \tag{94}$$

Since $n - 1 = 36m\,(36m^2 + 11m + 1)$, n is a Carmichael number.

Therefore, from our candidates (86) for O_i, and whether (85) holds or not, we determine if $3p - 2 = 18m + 1$ is an S prime. Sooner or later that will surely happen. Then (94) is a Carmichael solution. Here are three examples.

From $N = 4951 \cdot 9901$, which failed in -44, we find that 14851 is an S prime. Therefore,

$$C_7 = 4951 \cdot 9901 \cdot 14851 = 727993807201 \tag{95}$$

is acceptable for -44.

Similarly, in Perrin from O_7 we have

$$C_8 = 50647 \cdot 101293 \cdot 151939 = 779475417411169. \tag{96}$$

Also from Perrin we have

$$C_9 = 69991 \cdot 139981 \cdot 209971 = 2057172011015041. \tag{97}$$

Our 24 acceptable composites, nine C_i, ten O_i and five T_i, were all computed on a pocket calculator HP $-$ 41C. That makes it clear what could be done on a big machine.

(B) Are there acceptable composites common to -23 and -31, -23 and -44, etc? Almost certainly, but they should be very sparse. It would be instructive to know the

smallest -23, the smallest -31, the smallest -23 and -31, etc. It would be instructive to have complete tables up to some large M. That cannot be done on a HP $-$ 41C.

(C) Is it feasible to make such complete tables up to, say, $M = 10^{10}$ or larger? Presumably so. One would want to do a lot of preliminary sieving as we suggest in Section 4. If there are only a modest number of acceptable composites up to some big M, then one could use the algorithm for one or more $A(n)$ as a practical primality test. That would be like the Selfridge-Wagstaff test. There are many variations. We will not labor the point.

(D) The most important question before us is this: Is there an acceptable composite with a Q or I signature? We know of none for the -23, -31, or -44 $A(n)$. We do not know if they exist. We do not know how to construct them. *If* there really are none for -23, -31, and -44, that would be very important since the algorithm would give us an efficient, sufficient condition for $5/6$ of all primes. Use of two of these $A(n)$ would raise the fraction to $35/36$ and all three would suffice for $215/216$ of all primes. That is such an enticing possibility that we must investigate this question.

If we had the table referred to in (C), that could certainly help. If one or more such composites turned up we could analyze them and understand the problem better than we now do. If there were none, it might encourage us (even more) to prove that there are none at all. Absent a table, and since we cannot construct one on the aforementioned HP $-$ 41C, we return to the concept of the *outsider* in Section 4.

We had $x^3 - 7x^2 + 21x - 1 = 0$ there with an S prime 29 that has a period $W = 7$. Then $m = 9$ is an outsider for 29 since

$$m \cdot 29 \not\equiv k \cdot 7 \cdot 29 + 29,$$

and yet

$$A(-9 \cdot 29) \equiv A(-1), \quad A(9 \cdot 29) \equiv A(1) \pmod{29}.$$

In Section 16 we will learn how to construct composites $N = pq$, where p and q are S primes that are mutual outsiders of each other, and such that the signature of $N \pmod N$ is an I or Q signature. This is accomplished by forcing the roots of the cubic $(\mathrm{mod}\ N)$ to obey the power laws that they would obey (such as $a^N \equiv b$) if N were an I or Q prime. We can do that if we do *not* select the $A(n)$ in advance, but rather allow $A(1)$ and $A(-1)$ to take on any values needed by the construction. Consider two examples. Let

$$x^3 + 14x^2 + 126x - 1 = 0, \tag{98}$$

and let $N = 35 = 5 \cdot 7$. Here 5 is an S prime with $W = 4$ which has 7 as an outsider. Conversely, 7 is S with $W = 3$ and 5 as an outsider. The signature of $35 \pmod{35}$ is

$$3, \quad 126, \quad 14, \quad 14, \quad -14, \quad 3. \tag{99}$$

From (42a) we have

$$14 = B \equiv 70a + 14a^2 \pmod{35},$$

which with $a^3 + 14a^2 + 126a - 1 \pmod{35}$ is satisfied by $a = 1$. Then (42b, c) give us $A \equiv C \equiv 3$, as they are. So (99) *is* a Q signature since $14 \not\equiv 3 \pmod{35}$. But (99) is not an acceptable signature. The cubic in (98) has the discriminant $d = -4910611$,

and, since $(d/5) = (d/7) = +1$, obviously we also have $(d/35) = +1$, and not -1 as it should be.

It is clear that if N were the product of any number of S primes, for any $A(n)$, and if $N \pmod N$ has a Q signature, then N could never be acceptable since it could never have $(d/N) = -1$.

Now let us construct such an N with an I signature. That will not have the same defect if we stay clear of *ramified* S primes since we will have $(d/N) = +1$, as we should. Consider

$$x^3 - 862x^2 - 22x - 1 = 0 \tag{100}$$

and $N = 1537 = 29 \cdot 53$. Since $d = -2202681203 = -89 \cdot 24749227$, it is prime to N. Here, 29 is S with $W = 7$ and 53 as an outsider. And 53 is S with $W = 13$ and 29 as an outsider. The signature of $N \pmod N$ is

$$862, \quad -22, \quad 456, \quad 558, \quad 862, \quad -22. \tag{101}$$

Further, we have

$$\begin{aligned} 456 + 558 &\equiv 862(-22) - 3 \pmod{1537}, \\ \pm(-1435) &\equiv \sqrt{d} \pmod{1537}, \end{aligned} \tag{102}$$

in agreement with (46) and (47). So (101) is an I signature and $(d/1537) = +1$ as it should. From (102) we have

$$F = (1537, -1435, 358611). \tag{103}$$

(Note that we had to choose the odd -1435 and not its congruent $+102$ since d is odd. The discriminant of (x, y, z) is $y^2 - 4xz$ and is odd if, and only if, y is odd.)

Unlike our $d = -23$, -31, and -44 sequences, where $Q(\sqrt{d})$ had class number 3 and therefore only one S form and only two I forms, the present large d has $Q(\sqrt{d})$ with class number 15420. There are 5140 S forms and 10280 I forms, and (as always) the 5140 S forms comprise a subgroup under composition (of index 3) in the class group of order 15420. If there were no easier way, we would now have to check whether F, which is already reduced, satisfies

$$F \sim \text{one of 10280 } I \text{ forms}, \tag{104}$$

since (101) is now acceptable if, and only if, (104) is true.

We need not do that. The forms that represent the S primes 29 and 53 must be S forms and lie in the subgroup. They are

$$F_1 = (29, 15, 18988633) \quad \text{and} \quad F_2 = (53, 49, 10390017),$$

and the composition of F_1 and F_2 is F since [10]

$$1537 = 29 \cdot 53, \quad -1435 \equiv 15 \pmod{2 \cdot 29}, \quad -1435 \equiv 49 \pmod{2 \cdot 53}.$$

Therefore, F is also one of the 5140 S forms in the subgroup and any prime that it does represent, such as

$$445499 = 8^2 \cdot 1537 - 8 \cdot 1435 + 358611,$$

must be an S prime. Therefore, (104) fails and 1537 cannot be a prime.

It is now clear that if N were the product of any number of S primes, for any $A(n)$, then N could never be acceptable if it had an I signature since its F would always be equivalent to an S form.

We repeat: we know of no such Q or I signatures of $N \pmod N$ for the -23, -31, or -44 sequences, but, if there are any, the Jacobi symbol for Q signatures and the F-test for the I signatures will protect us against them. If such an N is square-free, as $N = 35$ and 1537 are, it is *essential* that there be outsiders in that $A(n)$. For if

$$N = p_1 \cdot p_2 \cdots p_n$$

with each p_i an S prime, and if

$$A(N) \equiv A(1), \quad A(-N) \equiv A(-1) \pmod{p_i}$$

for each i, and if there are no outsiders, then $W(p_i) \mid N - 1$ and the signature of $N \pmod{p_i}$ is an S signature for each i. Therefore, N has an S signature $(\bmod N)$ and cannot be either Q or I.

Since all Q and I composites that are divisible *only* by S primes are innocuous, we may now rephrase the question in (D). Are there any *other* Q or I composites? This is the next question. In [12] we answer this question using a powerful new method. See the end of Section 17 below.

We now return to our numerous S composites to decide what to do about them.

9. Quadratic Representations and the z-Test. In Section 6 we called C_1 acceptable since it does satisfy (12) and (21a). Nonetheless, it must be composite unless it has precisely one representation (23). Actually, we have an embarrassment of riches:

$$\begin{aligned} C_1 &= 11389^2 + 23 \cdot 17340^2 = 24683^2 + 23 \cdot 16728^2 \\ &= 43627^2 + 23 \cdot 14952^2 = 69763^2 + 23 \cdot 9732^2. \end{aligned} \tag{105}$$

Since each representation $u^2 + 23v^2$ gives us two square-roots for $\sqrt{-23} = \pm u/v$, C_1 cannot be prime. If we had a convenient algorithm for computing *all* the representations of

$$n = u^2 + 23v^2 \quad \text{and} \quad 8n = u^2 + 23v^2$$

very efficiently, say in $O(\log n)$ operations, we could add that to Perrin's $A(n)$ and thereby easily settle the primality of all S signatures. We know of no such algorithm.

Similarly, C_2 through C_9 each has four representations $C_i = u^2 + Nv^2$, where N is the appropriate value 23, 31, or 11. (Since C_4 has four factors, one might expect eight representations, but one of the four factors is the ramified 31. Its degenerate $31 = 0^2 + 1^2 \cdot 31$ does not double the number of representations.)

If p is *prime*, and if

$$mp = u^2 + Nv^2 \tag{106}$$

for certain m and any $N > 0$, there is a very efficient algorithm [5] for computing the unique solution. The first phase is the solution of

$$R^2 \equiv -N \pmod{p}. \tag{107}$$

Of course, for I primes p, we can read R directly from the signature, as in (47). But the S signature is uninformative, and we must compute (107) instead. Having $R^2 + N = Sp$, we have a quadratic form

$$(p, 2R, S) \tag{108}$$

of discriminant $-4N$. Reducing this to a reduced form then easily gives us (106). See [5].

If we use this algorithm for (106) with "p" $= C_1$, $N = 23$, $m = 1$, one of two events must occur: Either (1): the process breaks down and gives no solution, thereby revealing that C_1 is *not* a p, or (2): the process does work and gives us exactly one of the four solutions (105). A third possibility, that we obtain a solution of $8C_1 = u^2 + 23v^2$ instead, cannot happen in this case since C_1 is a product of S primes only.

The four solutions (105) are equally true, none has any special precedence, and if the second event occurs it seems almost contrary to the principles of Thomas Jefferson. Nonetheless, that is what happens: the algorithm for (106) gives us

$$R = 1415929016$$

for (107) and therefore

$$C_1 = 43627^2 + 23 \cdot 14952^2$$

for (106).

Let us analyze this curious outcome. If $p = 2^s(2k + 1) + 1$, the first step in the solution of (107) is the evaluation of

$$R_0 \equiv (-N)^{k+1} \quad \text{and} \quad N_0 \equiv (-N)^{2k+1} \pmod{p}. \tag{109}$$

They satisfy

$$R_0^2 \equiv -NN_0. \tag{110}$$

If it happens that $N_0 \equiv 1 \pmod{p}$, the algorithm terminates (abruptly) and R_0 is obviously the required solution. If $N_0 \not\equiv 1$, the algorithm selects the smallest z for which $(z/p) = -1$, computes

$$c_0 = (z)^{2k+1}, \tag{111}$$

and now enters its main routine. This utilizes the cyclic group of residues prime to p (mod p). It is *only* in this main routine that the primality of p is involved via this cyclic group of order $p - 1$.

What happened above is that

$$C_1 = 2^3(880656015) + 1$$

gives us

$$N_0 \equiv 1 \quad \text{and therefore} \quad R_0 \equiv (-23)^{440328008} = R.$$

This R is an authentic $\sqrt{-23}$ for the modulus C_1—that is, it is one of the eight. Then, this R gives us one representation via the form (108), and the lack of primality of C_1 did not enter at all.

Surprisingly, the same thing ($N_0 \equiv 1$) happens with C_2, and we obtain

$$C_2 = 70243^2 + 23 \cdot 10098^2,$$

one of the four representations. (Find the other three if you are interested.) Also, it happens with C_6, and we obtain

$$C_6 = 12689^2 + 11 \cdot 12330^2.$$

The other three, even if you are not interested, are

$$27505^2 + 11 \cdot 9894^2 = 34865^2 + 11 \cdot 7494^2 = 41761^2 + 11 \cdot 2850^2.$$

But with C_3 we have event (1) instead: breakdown! Here

$$N_0 \equiv (-31)^{(C_3-1)/8} \equiv -10263692081 \pmod{C_3},$$

and now the main routine is engaged. Then $z = 11$ is the first solution of $(z/C_3) = -1$ and (111) is evaluated:

$$c_0 \equiv -2867119581 \pmod{C_3}. \tag{112}$$

The algorithm then gets into an infinite loop, essentially because $c_0^2 \equiv 1 \pmod{C_3}$. Obviously, that could not happen if C_3 were prime since then $\sqrt{1}$ could only be ± 1. We say C_3 is not an Euler 11-pseudoprime and is not a strong 11-psp (pseudoprime). We may note that C_3 is also not a strong (-31)-psp although this time it is an Euler (-31)-psp. (See [7], [11] for these definitions.) Any of these three failures implies that C_3 is composite, but the actual breakdown here was caused by z.

If n has an S signature and z is the smallest solution of $(z/n) = -1$, a test whether n is a strong z-psp will be called the *z-test*.

In C_1, C_2, and C_6 we had $N_0 \equiv 1$ above, and we did obtain a representation. However, in all six $C_i < 25 \cdot 10^9$, C_i fails its z-test: it is not a strong z-psp, and therefore it cannot be prime. (We did not test the large C_7, C_8, C_9. They were computed much later.)

In the Owings composites, O_1 and O_2, we again had $N_0 \equiv 1$ and obtained one of the two representations:

$$O_1 = 4438^2 + 23 \cdot 1083^2, \quad O_2 = 17072^2 + 23 \cdot 5433^2.$$

But again O_1 and O_2 failed the z-test, for example, for O_2, $z = 3$ and

$$3^{(O_2-1)/2} \equiv 88107, \quad 3^{O_2-1} \equiv 1 \pmod{O_2}. \tag{113}$$

Likewise, all five T_i fail their z-test, so that all of these S composites: C_1, C_2, C_3, C_4, C_5, C_6, O_1, O_2, T_1, T_2, T_3, T_4, T_5 can be shown to be composite merely with the relatively simple z-test, and without even becoming involved in the algorithm for (106).

Nonetheless, there are two convincing reasons why the z-test will not work on *every* S composite. In the first place, if $N_0 \equiv 1$, and this occurs frequently, (111) is not computed, and z has no real functional relevance to the situation. Secondly, the choice of the *smallest* solution of $(z/n) = -1$ is merely one of convenience: there is no known correlation between the *size* of z and whether a composite n is, or is not, a strong z-psp. Since it is not possible to rebut these arguments, the easiest way of settling the question is to find a counterexample. We therefore computed the additional O_i in (89) and (90).

With these eight new S-composites, we obtained these results: First, O_3, O_6, O_7, and O_8 also fail their z-tests, as before. But

$$O_4 = 24379 \cdot 48757 = 1188646903 \tag{114}$$

is the counterexample, and so we record the details.

$$N_0 \equiv (-11)^{(O_4-1)/2} \equiv 1, \quad \text{and therefore} \quad R_0 \equiv 346290683 \equiv \sqrt{-11}$$

gives us one (of the two) representations

$$O_4 = 15182^2 + 11 \cdot 9333^2.$$

So $z = 3$ was never used but

$$3^{(O_4-1)/2} \equiv -1 \pmod{O_4},$$

and O_4 *is* a strong 3-psp. Thus, O_4 has an S signature, passes the Jacobi symbol test, has an authentic $\sqrt{-11}$ and representation, and passes its z-test.

Of course, O_4 is not prime. Its "next" z after 3 is 5 and

$$5^{O_4-1} \equiv -97515 \pmod{O_4},$$

and so O_4 is not even a 5-psp, let alone a strong 5-psp. Or again, the other representation

$$O_4 = 6598^2 + 11 \cdot 10203^2$$

also proves O_4 to be composite.

The large O_{10} (see (90)) is just like O_4 in these respects: $N_0 \equiv 1$, $z = 3$, and $3^{(O_{10}-1)/2} \equiv -1$. It also passes the z-test.

The remaining two O_i, namely O_5 and O_9, also pass the z-test, both with $z = 2$, but they are not as deceptive as O_4 and O_{10} were. Both O_5 and O_9 have $N_0 \not\equiv 1$, and in both cases the algorithm for (107) gets into an infinite loop, not because of the c_0 in (111), but because these O_i are not strong or even Euler $(-N)$-psp for $N \equiv 11$ and 23, respectively. Thus, no $\sqrt{-N}$ or representations are obtained, and if this algorithm (107) were computed besides the z-test, we would know that O_5 and O_9 are also composite.

However one rates the last two cases, O_5 and O_9, O_4 and O_{10} definitely pass all tests in this section, and we now turn to another test for n having S signatures.

10. A Test Passed By. The I signature gives us $\sqrt{d}$; the S signature does not. The Q signature gives us one root of the cubic; the S signature does not. Actually, in most cases, this latter information did appear but it was allowed to go by unrecorded. Suppose $p = 2^s(2k + 1) + 1$ is an odd S prime. Its signature was obtained from that of $(2k + 1)$ by doubling this argument $(s - 1)$ times, and then by $2((p - 1)/2) + 1$ as a final step. Previously, these earlier signatures (and *they* had the information) were written over and destroyed. Let us examine them for five S primes in Perrin. Instead of listing the final signature for p, we list that of $(p - 1)$ instead. It has a notable repetition:

(115) $$A(-1),\ 3,\ A(1),\ A(-1),\ 3,\ A(1).$$

n	Signature of $n \pmod p$						p
29	31,	−1,	8,	31,	−1,	8	59
58	−1,	3,	0,	−1,	3,	0	59
$\overline{25}$	66,	80,	79,	45,	19,	83	$\overline{101}$
50	92,	−1,	40,	92,	−1,	40	101
100	−1,	3,	0,	−1,	3,	0	101
$\overline{43}$	12,	1,	141,	49,	1,	137	$\overline{173}$
86	62,	−1,	105,	62,	−1,	105	173
172	−1,	3,	0,	−1,	3,	0	173
$\overline{2415}$	9481,	−1,	1708,	9481,	−1,	1708	$\overline{9661}$
4830	−1,	3,	0,	−1,	3,	0	9661
9660	−1,	3,	0,	−1,	3,	0	9661
$\overline{11013}$	−1,	3,	0,	−1,	3,	0	$\overline{22027}$
$\underline{22026}$	−1,	3,	0,	−1,	3,	0	$\underline{22027}$

For 59, 101 and 173, the period W does not divide $(p-1)/2$, and the signature of $(p-1)/2$ is of the form

(116) $$e, \quad -1, \quad f, \quad e, \quad -1, \quad f.$$

Here, -1, like the 3 found below it, is one of the two roots of

(117) $$x^2 - 2x \equiv 3 = A(0) \pmod{p},$$

and we will presently analyze the specific information in e and f.

The period of 9661 (which divides O_1) divides $(p-1)/2$ but not $(p-1)/4$. Its characteristic signature (116) comes one inning earlier. The period of 22027 (which divides O_2) is *odd* and no signature (116) occurs. This S prime is uninformative in this respect. (Information of another type is found at $(p-1)/3$.)

Since (116) gives (115) by the Doubling Rule, we have

(118) $$f^2 - 2e \equiv A(2), \quad e^2 - 2f \equiv A(-2),$$

in addition to the (117) satisfied by $x = -1$. Therefore, we have

(119) $$f^4 - 2A(2)f^2 - 8f + A^2(2) - 4A(-2) \equiv 0,$$

(120) $$e^4 - 2A(-2)e^2 - 8e + A^2(-2) - 4A(2) \equiv 0.$$

Now write

(121) $$f = 2g - A(1)$$

in (119), and its left side becomes

(122) $$16(g - A(1))(g^3 - A(1)g^2 + A(-1)g - 1),$$

so the four roots of (119) are

(123) $$f_0 = A(1) \quad \text{and} \quad f_i = 2g_i - A(1) \qquad (i = 1,2,3),$$

where the g_i are the three roots of

$$x^3 - A(1)x^2 + A(-1)x - 1 \equiv 0 \pmod{p}.$$

Conversely,

(124) $$g_1 \equiv \frac{f + A(1)}{2}$$

gives us one root from the f in (116).

Interchange of $A(1)$ and $A(-1)$ gives us the four roots of (120):

(125) $$e_0 = A(-1) \quad \text{and} \quad e_i = \frac{2}{g_i} - A(-1) \qquad (i = 1,2,3).$$

Therefore,

(126) $$g_1 \equiv \frac{2}{e + A(-1)}$$

from the e in (116). But this is the same root in (124) since, from (118), we have

$$\frac{f + A(1)}{2} = \frac{e - A(-1)}{f - A(1)} = \frac{2}{e + A(-1)}.$$

Unlike the paradox about T. Jefferson in Section 9, it is easy enough to characterize the root of the cubic singled out by g_1. Since $g_1 g_2 g_3 \equiv 1$, either they are

all quadratic residues of p, (as occurs above in 9661 and 22027), or exactly one is (as in 59, 101 and 173). It is easy to prove that in this case g_1 is the quadratic residue. In fact, the 3 and the -1 both arise as

$$\left(\frac{g_1}{p}\right) + \left(\frac{g_2}{p}\right) + \left(\frac{g_3}{p}\right),$$

and the proof relates to the evaluation of that sum.

Let us pursue the characterization of g_1 back one more inning. In 9661, g_1, g_2, and g_3 are all quadratic residues, but $g_1 \equiv \frac{1}{2}(1708)$ is the only *quartic* residue among the three. In 173, the 1 standing above -1 is the only solution of $x^2 - 2x \equiv -1$, and it occurs if, and only if, g_1 is a quartic residue of p. In 101, where $g_1 \equiv 20$ is a quadratic but not a quartic residue, one finds $-1 + 2i$ and $-1 - 2i$ standing above -1 instead. Therefore, $\pm i \equiv \pm 10 \pmod{101}$. We will use this characterization presently.

Therefore, unless the S prime has an odd period, as $p = 22027$ does, we easily obtain one root g_1 and perhaps some other information from these penultimate signatures.

Now consider C_1 instead of an S prime. We find these signatures (mod C_1)

at $(C_1 - 1)/4$	X,	Y,	Z,	X,	Y,	Z,
at $(C_1 - 1)/2$	-1,	3,	0,	-1,	3,	0,
at $(C_1 - 1)$	-1,	3,	0,	-1,	3,	0,

where

$$X = 5208849706, \quad Y = 5157361904 \quad \text{and} \quad Z = 246283384.$$

Now Y is a solution of

$$x^2 - 2x \equiv 3 \pmod{C_1}$$

but is not congruent to -1 or 3 (mod C_1). Therefore, C_1 is composite, since a prime can only have those two roots. What is happening here is due to

$$Y \equiv -1 \pmod{821}, \quad Y \equiv 3 \pmod{1231}, \quad Y \equiv 3 \pmod{6971},$$

where these are the three primes dividing C_1. But 821 attains 3 one inning after 1231 and 6971 are already at this fixed point. This "misalignment" gives us a $Y \not\equiv -1, 3 \pmod{C_1}$ and it proves C_1 to be composite.

In a Carmichael solution such a misalignment is quite probable since there are at least three prime factors. In fact, the same test works on C_2 through C_6. (We did not try the larger $C_7 - C_9$.) For the record, the corresponding values of $Y \pmod{C_i} \not\equiv -1$ or 3 are:

at $(C_2 - 1)/4$,	$Y \equiv 434194322$,
at $(C_3 - 1)/4$,	$Y \equiv 4640837320$,
at $(C_4 - 1)/4$,	$Y \equiv 6135985282$,
at $(C_5 - 1)/8$,	$Y \equiv 17046671936$,
at $(C_6 - 1)/4$,	$Y \equiv 1454557351$.

We have no assurance that this easy test will work on all C_i. That seems very unlikely.

The test may or may not work on the T_i, which have only two factors instead of three or more. We find that T_1 and T_5, like the C_i, have a $Y \not\equiv -1$ or 3 and are exposed as composites. But T_2, T_3, and T_4 pass the test and T_2 and T_4 actually give us a valid root g_1 of the cubic, while T_3, like $p = 22027$ in the table, is uninformative.

The O_i are quite likely to pass the test (unlike the C_i) since they have only two factors, and they tend to be aligned because of the condition (85) that $2p - 1$ must satisfy. In fact, O_1, O_2, O_3, O_6, O_8, and O_9 all pass the test (i.e., are not exposed as composites), while O_7 fails ($Y \not\equiv -1$ or 3).

The remaining three we list for special mention:

	z-test	Test Passed By
O_{10}	passed	failed
O_5	$\frac{1}{2}$passed	$\frac{1}{2}$failed
O_4	passed	passed

O_{10}, which, unlike most O_i, passed the z-test, now, unlike most O_i, gets caught by the new test. It is the most contrary of our examples.

O_5, which passed its z-test, but failed to obtain a $\sqrt{-11}$ or a representation $O_5 = u^2 + 11v^2$, is equally complicated in the new test. Consider its signatures:

at $(O_5 - 1)/4$	X_1	Y_1	Z_1	X_2	Y_2	Z_2
at $(O_5 - 1)/2$	e	-1	f	e	-1	f
at $(O_5 - 1)$	-1	3	1	-1	3	1

with

$$e = 1831432868, \qquad f = 746855451,$$
$$Y_1 = 1368191032, \qquad Y_2 = 689901363.$$

It appears to pass at $(O_5 - 1)/2$. The -1 there shows that its two factors 32077 and 64153 are not misaligned. And f gives us an authentic root $g_1 = 373427726$. But $Y_1 + Y_2 \equiv 256614 \not\equiv +2$ or $-2 \pmod{O_5}$. If O_5 were prime, we would have $+2$ for this sum, if, like 173 in the table, g_1 were a quartic residue, and we would have -2, if, like 101 in the table, g_1 is not a quartic residue. Therefore O_5 is composite; its two factors are not misaligned, they are aligned, but each is in his own space and doing his own thing. It is true that g_1 is a root and a square $(\text{mod } O_5)$. In fact, it has four square roots:

$$\sqrt{g_1} \equiv \pm 297803208, \qquad \pm 341427248.$$

O_5 is the most subtle and complex of our examples.

O_4, which was the first to pass the z-test, obtained a $\sqrt{-11}$ and a representation, now also passes the new test and obtains an authentic root, $g_1 \equiv 818715002$, of its cubic. O_4 is the most deceptive of our examples.

It is a tribute to the strength of our $A(n)$ that the rareness of their acceptable composites allows us to attribute individual personalities to these composites; no one ever thought of assigning personalities to Wagstaff's 21853 2-pseudoprimes.

The test in this section is very similar to that of a strong psp. Our extra roots $Y \not\equiv -1$ or 3 are entirely analogous to the $88107 \equiv \sqrt{1}$ that we saw in (113).

11. The S Signatures. If we confine the factors of a composite to S primes, we obtain a full panoply of pseudoprime-like acceptable S-composites, including Carmichaels and analogs of strong-psp. A big advantage of our $A(n)$ is that the number of such composites is much reduced because the density of S primes is only $1/6$. But within this reduced population these composites behave just like psp. Tests, such as those in Sections 9 and 10, expose most of them as composites, but some get through. We saw that O_4 in (89) passes both of these tests.

One can easily eliminate all (of the many) O_i: Upon obtaining an S signature for n, determine if $8n + 1$ is a perfect square. If

$$8n + 1 = (4k \pm 1)^2 \qquad (k > 1),$$

then $n = k(2k \pm 1)$ is obviously composite.

But it is unlikely that even all three tests, taken together, could catch all S-composites. This is our recommendation for n that have S signatures. There are three cases:

(A) We have some a priori reason to believe that n is composite.

(B_1) We have no such reason but n is, in fact, composite.

(B_2) We have no such reason and n is, in fact, prime.

If we are in (A), it certainly does no harm to use any, or all, of these three tests and n will probably be exposed. If we are in (B) (the usual case), we really do not recommend the use of the tests in Sections 9 and 10 since they are always inconclusive if we are in (B_2). If the intent is to use some strong test to delete most of the composites, then our recommendation is to switch to another of our $A(n)$. After all, that is the claim in our title: These are very strong tests.

This is what we can expect. In (B_1), with a very high probability, the new signature will not even be slightly acceptable. For example, O_4, that is so deceptive in the -44 $A(n)$, has this signature

$$27603213, \quad 770199562, \quad 272340289, \quad 272340289, \quad 763623965, \quad 574664267$$

in Perrin. With a small probability in (B_1), we may find another S-signature in this second $A(n)$. In that case, try a third $A(n)$.

If we are in (B_2), with a probability of $5/6$ we will obtain an I or Q signature in the second $A(n)$. Of course, this brings us back to our unresolved main question Section 8(D). Pending a solution of this question we can only say that, with a high probability, n is prime. In the $1/6$ of the cases where we get another S signature, try a third $A(n)$.

12. Theory. Setting Up a General Cubic Recurrence. In this and the following sections we will prove and generalize the results stated in the previous sections. Although some of these results occur in the literature, we include their proofs here both for ease of reading and because they cost little extra effort.

For simplicity we restrict ourselves to cubic recurrences of integers whose reverse sequence consists of integers also. That is, let r, s be integers (in $\mathbf{Z}$) and consider the recurrence

$$A(n + 3) = rA(n + 2) - sA(n + 1) + A(n). \tag{127}$$

This paper is concerned only with the special recurrence defined by the initial conditions:

$$A(-1) = s, \quad A(0) = 3, \quad A(1) = r. \tag{128}$$

Consider the associated characteristic polynomial for (127)

$$f(X) = X^3 - rX^2 + sX - 1. \tag{129}$$

(When more than one sequence is being considered we will denote $A(n)$ by $A_f(n)$ if necessary.) Let $f(X) = (X - \alpha)(X - \beta)(X - \gamma)$ for the appropriate complex numbers α, β, γ, and let $d = d_f = [(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)]^2$ denote the discriminant of f. Let $K = \mathbf{Q}(\alpha, \beta, \gamma) = \mathbf{Q}(\alpha, \sqrt{d})$ denote the splitting field of f over the rational numbers $\mathbf{Q}$. Let I_K denote its ring of integers. We note that since we have made no assumption on the character of the roots of f other than those implied by its form (129), we see that our theory contains the theory for certain second-order recurrences.

From the theory of linear recurrences it is known that $A(n)$ is a linear combination of α^n, β^n, γ^n. Then, from the initial conditions (128), we see that we are dealing with the special case

$$A(n) = \alpha^n + \beta^n + \gamma^n. \tag{130}$$

We first make the trivial observation that $A_f(-n) = A_g(n)$, where g is the reciprocal polynomial for f:

$$g(X) = X^3 - sX^2 + rX - 1.$$

Thus the results proved for $n > 0$ hold, properly interpreted, for $n < 0$ as well. More generally set, for any integer m,

$$\begin{aligned} f_m(X) &= (X - \alpha^m)(X - \beta^m)(X - \gamma^m) \\ &= X^3 - A_f(m)X^2 + A_f(-m)X - 1. \end{aligned} \tag{131}$$

We see that for all integers n,

$$A_f(mn) = A_{f_m}(n).$$

Thus again, with proper interpretation, results we prove for all $A(n)$ hold equally well for $A(mn)$; the special case $m = -1$ was given above.

For example, let p be any prime. Then, working mod pI_K and using Fermat's Little Theorem, we have

$$A(1) \equiv A(1)^p = (\alpha + \beta + \gamma)^p = \sum_{\substack{i+j+k=p \\ i,j,k \geq 0}} \frac{p!}{i!j!k!} \alpha^i \beta^j \gamma^k$$

$$\equiv \alpha^p + \beta^p + \gamma^p = A(p) \pmod{pI_K},$$

since $p \mid p!/i!j!k!$ unless one of i, j, $k = p$. Thus $A(p) \equiv A(1) \pmod{p}$ (as integers). Invoking the remark above we obtain the important congruence (71): for all integers m

$$A(mp) \equiv A(m) \pmod{p}. \tag{132}$$

With $m = \pm 1$, this was the starting point for our signatures in Section 1.

It follows, for example, from (132) that if n is a square free integer, then $A(n) \equiv A(1) \pmod{n}$ if, and only if, for all primes $p \mid n$, $A(n/p) \equiv A(1) \pmod{p}$.

13. General Signatures. In this section we gather together all of the general material on signatures needed to prove the results stated above about the signatures of primes and also to construct examples of composites having prescribed signatures. We recall that the sequence of six numbers $A(-n-1)$, $A(-n)$, $A(-n+1)$, $A(n-1)$, $A(n)$, $A(n+1)$ read mod m is defined to be the *signature of* n mod m.

Definition 1. (i) *We say that n has an S signature* mod m *provided the signature of n* mod m *is*

$$A(-2),\quad A(-1),\quad A(0),\quad A(0),\quad A(1),\quad A(2),$$

that is:

$$s^2-2r,\quad s,\quad 3,\quad 3,\quad r,\quad r^2-2s. \tag{133}$$

(ii) *We say that n has a Q signature* mod m *provided the signature of n* mod m *is*

$$A,\quad s,\quad B,\quad B,\quad r,\quad C, \tag{134}$$

where for some integer a satisfying $f(a)\equiv 0 \pmod m$ *we have*

$$A\equiv a^{-2}+2a,\quad B\equiv -ra^2+(r^2-s)a,\quad C\equiv a^2+2a^{-1} \pmod m. \tag{135}$$

(iii) *We say that n has an I signature* mod m *provided the signature of n* mod m *is*

$$r,\quad s,\quad D',\quad D,\quad r,\quad s, \tag{136}$$

where

$$D'+D\equiv rs-3,\quad (D'-D)^2\equiv d \pmod m. \tag{137}$$

We note that for technical reasons there are slight differences between the definitions given in Sections 1, 3 and the equivalent ones given here. First, we have not now included the restrictions that $D\not\equiv D' \pmod m$ and $B\not\equiv 3 \pmod m$ as they follow from (137) and (135), respectively (see Proposition 5). Second, we note that (137) immediately gives

$$D^2-(rs-3)D+\frac{(rs-3)^2-d}{4}\equiv 0 \pmod m \tag{138}$$

which is the relation (13a), (36) or (60) for $d=-23, -31, -44$, respectively. Finally, in the definition of a Q signature, it is more convenient in the theory to use the relations (42), as we already stated in Section 3. For completeness, we record the general relations in a Q signature corresponding to (14), (37), and (56):

$$\begin{aligned} B^3-rsB^2+(r^3+s^3-3rs)B+(r^3+s^3-r^2s^2)&\equiv 0 \pmod m,\\ (s^3-r^3)A&\equiv (s^2-3r)B^2+s(4r^2-s^2r-3s)B\\ &\quad +(s^5-3s^3r+6sr^2-2r^4) \pmod m, \end{aligned} \tag{138a}$$

and the formula for C is obtained from that for A by interchanging r and s. These relations immediately give the convenient linear relation

$$(r^2-3s)A+(rs-9)B+(s^2-3r)C\equiv r^2s^2-3rs-r^3-s^3 \pmod m.$$

We begin the derivations with the following lemma:

LEMMA 2. *Let* m, n *be integers such that* $\gcd(m,2d)=1$. *Let* $\mathfrak{A}$ *be an ideal of* K *such that* $\mathfrak{A}\cap\mathbf{Z}=m\mathbf{Z}$ (*e.g.* $\mathfrak{A}=mI_K$). *Then* $A(n-1)$, $A(n)$, $A(n+1)$ mod m *has*

one of the following shapes:

$$(139)\qquad \begin{array}{llll} & A(n-1) & A(n) & A(n+1) \\ S & 3 & r & r^2-2s \\ Q & B & r & C \quad \textit{where} \quad B \equiv -r\alpha^2 + (r^2-s)\alpha, \\ & & & \qquad C \equiv \alpha^2 + 2\alpha^{-1} \pmod{\mathfrak{A}} \\ I & D & r & s \quad \textit{where} \quad D \equiv \tfrac{1}{2}(rs-3-\delta) \pmod{\mathfrak{A}}, \\ & & & \qquad \delta = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha) \end{array}$$

for rational integers B, C, D if and only if the following conditions hold, respectively,

$$(140)\qquad \begin{array}{lll} S & \alpha^n \equiv \alpha, & \beta^n \equiv \beta, \quad \gamma^n \equiv \gamma \pmod{\mathfrak{A}}, \\ Q & \alpha^n \equiv \alpha, & \beta^n \equiv \gamma, \quad \gamma^n \equiv \beta \pmod{\mathfrak{A}}, \\ I & \alpha^n \equiv \beta, & \beta^n \equiv \gamma, \quad \gamma^n \equiv \alpha \pmod{\mathfrak{A}}. \end{array}$$

Proof. Let

$$\Delta = \begin{bmatrix} \alpha & \beta & \gamma \\ 1 & 1 & 1 \\ \alpha^{-1} & \beta^{-1} & \gamma^{-1} \end{bmatrix},$$

$$V_S = \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}, \quad V_Q = \begin{bmatrix} \alpha \\ \gamma \\ \beta \end{bmatrix}, \quad V_I = \begin{bmatrix} \beta \\ \gamma \\ \alpha \end{bmatrix}, \quad V_n = \begin{bmatrix} \alpha^n \\ \beta^n \\ \gamma^n \end{bmatrix}$$

and U_T (for $T = S, Q, I$) be the column vector of the appropriate row of (139) read backwards. Then, since $\delta^2 = d$ and so $\det \Delta = \delta$ is a unit mod $\mathfrak{A}$, we have $\Delta V_n \equiv \Delta V_T \pmod{\mathfrak{A}}$ if, and only if, $V_n \equiv V_T \pmod{\mathfrak{A}}$ $(T = S, Q, I)$. Moreover, $\mathfrak{A} \cap \mathbf{Z} = m\mathbf{Z}$ implies $\Delta V_n \equiv \Delta V_T \pmod{\mathfrak{A}}$ if, and only if, $\Delta V_n \equiv \Delta V_T \pmod{m}$. Thus, in order to prove the lemma, it suffices to show that $\Delta V_T = U_T$ $(T = S, Q, I)$. For $T = S$, this is immediate. Moreover, the middle entry of ΔV_T for any T is $\alpha + \beta + \gamma = r$. So it remains to verify the first and third entry when $T = Q, I$. The first entry of ΔV_Q is $\alpha^2 + 2\beta\gamma = \alpha^2 + 2\alpha^{-1}$; the third is $1 + \gamma\beta^{-1} + \beta\gamma^{-1} = 1 + \alpha(\beta^2 + \gamma^2) = 1 + \alpha(A(2) - \alpha^2) = -r\alpha^2 + (r^2 - s)\alpha$ since $\alpha^3 = r\alpha^2 - s\alpha + 1$. The first entry of ΔV_I is $\alpha\beta + \beta\gamma + \gamma\alpha = \gamma^{-1} + \alpha^{-1} + \beta^{-1} = A(-1) = s$. Finally, the third entry D_1 of ΔV_I is $D_1 = \beta\alpha^{-1} + \gamma\beta^{-1} + \alpha\gamma^{-1} = \beta^2\gamma + \gamma^2\alpha + \alpha^2\beta$. Set $D_1' = \alpha\beta^{-1} + \beta\gamma^{-1} + \gamma\alpha^{-1} = \alpha^2\gamma + \alpha\beta^2 + \beta\gamma^2$. We see that

$$\begin{aligned} D_1' + D_1 &= \alpha(\beta^2 + \gamma^2) + \beta(\alpha^2 + \gamma^2) + \gamma(\alpha^2 + \beta^2) \\ &= -A(3) + A(1)A(2) = rs - 3, \end{aligned}$$

and

$$D_1' - D_1 = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = \delta.$$

Solving these equations gives the desired result $D_1 = \frac{1}{2}(rs - 3 - \delta)$. □

THEOREM 3. *Let m, n be integers such that* $\gcd(m, 2d) = 1$. *Then*

(i) *n has an S signature* mod *m if, and only if,*

$$(141)\qquad \alpha^n \equiv \alpha, \quad \beta^n \equiv \beta, \quad \gamma^n \equiv \gamma \pmod{mI_K}.$$

(ii) *n has a Q signature* mod m *if, and only if, for all prime ideals $\mathfrak{P}$ of K such that $\mathfrak{P} \mid m$ (write $\nu = \operatorname{ord}_{\mathfrak{P}} m$) we have one of the three congruences*

$$(142)\qquad \begin{cases} \alpha^n \equiv \alpha, & \beta^n \equiv \gamma, & \gamma^n \equiv \beta \pmod{\mathfrak{P}^\nu}, \\ \beta^n \equiv \beta, & \alpha^n \equiv \gamma, & \gamma^n \equiv \alpha \pmod{\mathfrak{P}^\nu}, \\ \gamma^n \equiv \gamma, & \alpha^n \equiv \beta, & \beta^n \equiv \alpha \pmod{\mathfrak{P}^\nu}. \end{cases}$$

(iii) *n has an I signature* mod m *if, and only if, for all prime ideals $\mathfrak{P}$ of K such that $\mathfrak{P} \mid m$ (write $\nu = \operatorname{ord}_{\mathfrak{P}} m$) we have either*

$$(143)\qquad \alpha^n \equiv \beta, \quad \beta^n \equiv \gamma, \quad \gamma^n \equiv \alpha \pmod{\mathfrak{P}^\nu}$$

or

$$(144)\qquad \alpha^n \equiv \gamma, \quad \gamma^n \equiv \beta, \quad \beta^n \equiv \alpha \pmod{\mathfrak{P}^\nu}.$$

The complications in the statements of the criterion for Q and I signatures will be discussed following the proof of Theorem 6.

Proof. Applying Lemma 2 both to the original sequence and to the reverse sequence (interchanging r and s), we immediately obtain the result for the S signature.

We now prove (ii). First assume n has a Q signature mod m. We have

$$0 \equiv f(a) = (a-\alpha)(a-\beta)(a-\gamma) \pmod{\mathfrak{P}^\nu}.$$

Since $\gcd(m, 2d) = 1$, we see $\mathfrak{P}^\nu$ may only divide one factor, say the first. Hence $\alpha \equiv a \pmod{\mathfrak{P}^\nu}$. Substituting α for a in the congruences (135), we obtain congruences mod $\mathfrak{A} = \mathfrak{P}^\nu$ which from Lemma 2 yields the first alternative in (142). Of course, $\beta \equiv a \pmod{\mathfrak{P}^\nu}$ or $\gamma \equiv a \pmod{\mathfrak{P}^\nu}$ yield the other two possibilities in (142). Conversely, assume one of the possibilities in (142) holds, say the first, for some prime ideal $\mathfrak{P}$ of K, $\mathfrak{P} \mid m$. Applying Lemma 2 with $\mathfrak{A} = \mathfrak{P}^\nu$, we obtain the relations in (139Q). We also have the condition (140Q) with α, β, γ replaced by $\alpha^{-1}, \beta^{-1}, \gamma^{-1}$, respectively, and so we obtain (139Q) with n replaced by $-n$ and α by α^{-1}. Looking at the proof of Lemma 2, we see $B \equiv 1 + \beta\gamma^{-1} + \beta^{-1}\gamma$ which is symmetric in replacing α, β, γ by $\alpha^{-1}, \beta^{-1}, \gamma^{-1}$, and so $A(-n+1) \equiv A(n-1) \pmod{\mathfrak{P}^\nu}$. We now see we have obtained (135), with α replacing a, and $\mathfrak{P}^\nu$ replacing m. Using these congruences, we solve for $\alpha \bmod \mathfrak{P}^\nu$. We have

$$\begin{aligned} B &\equiv (r^2 - s)\alpha - r\alpha^2 \pmod{\mathfrak{P}^\nu}, \\ C &\equiv 2\alpha^{-1} + \alpha^2 \pmod{\mathfrak{P}^\nu}, \\ s &\equiv \alpha^{-1} + r\alpha - \alpha^2 \pmod{\mathfrak{P}^\nu}, \end{aligned}$$

and so $(r^2 - 3s)\alpha \equiv 3B - 2rs + rC \pmod{\mathfrak{P}^\nu}$. Since $B \equiv A(-n+1) \pmod{\mathfrak{P}^\nu}$, we also have

$$\begin{aligned} B &\equiv (s^2 - r)\alpha^{-1} - s\alpha^{-2} \pmod{\mathfrak{P}^\nu}, \\ A &\equiv 2\alpha + \alpha^{-2} \pmod{\mathfrak{P}^\nu}, \\ r &\equiv \alpha + s\alpha^{-1} - \alpha^{-2} \pmod{\mathfrak{P}^\nu}, \end{aligned}$$

and so $(s^2 - 3r)\alpha \equiv -sB - rA + r(s^2 - r) \pmod{\mathfrak{P}^\nu}$. One or the other of these congruences may be solved for α to obtain $\alpha \equiv a \pmod{\mathfrak{P}^\nu}$ for a rational integer $a_{\mathfrak{P}}$, provided $\mathfrak{P} \nmid r^2 - 3s$ or $\mathfrak{P} \nmid s^2 - 3r$. In case $\mathfrak{P} \mid r^2 - 3s$ and $\mathfrak{P} \mid s^2 - 3r$ we have, for the prime rational integer p such that $p\mathbf{Z} = \mathfrak{P} \cap \mathbf{Z}$, that either $r \equiv s \equiv 0$ or $3 \pmod{p}$ or for $p \equiv 1 \pmod 3$ and h a primitive cube root of $1 \bmod p$ we have $r \equiv 3h$, $s \equiv 3h^2 \pmod{p}$ or $r \equiv 3h^2$, $s \equiv 3h \pmod{p}$. It is immediately verified that the last three cases violate the hypothesis that $p \nmid d$ (i.e. $\gcd(2d, m) = 1$). In the first case we have $f(X) \equiv X^3 - 1 \pmod{p}$, and so $f(1) \equiv 0 \pmod{p}$ and $p \neq 3$ (or else $p \mid d$). We easily see then that there is a rational integer b such that $f(b) \equiv 0 \pmod{p^\nu}$, and, as above, we see either $\alpha \equiv b$ or $\beta \equiv b$ or $\gamma \equiv b \pmod{\mathfrak{P}^\nu}$. Since the first alternative in (142) holds, we see in all three cases there is a rational integer $a_{\mathfrak{P}}$ so that $\alpha \equiv a_{\mathfrak{P}} \pmod{\mathfrak{P}^\nu}$. We have now established that the relation (135) holds with a replaced by $a_{\mathfrak{P}}$ and m replaced by $\mathfrak{P}^\nu$ for all $\mathfrak{P} \mid m$. Since the congruence involves only rational integers, we see (135) holds with a replaced by an integer a_p and m by p^ν for all $p \mid m$ ($\nu = \operatorname{ord}_p m$). Finally, by the Chinese Remainder Theorem we obtain (135) itself.

Finally we prove (iii). First, assume n has an I signature mod m. Let $\mathfrak{P}$, ν be as in the statement of the theorem. From (137), $\delta^2 = d$ and $\mathfrak{P}^\nu \mid m$ we see that

$$\mathfrak{P}^\nu \mid (D' - D - \delta)(D' - D + \delta).$$

Since $\gcd(m, 2d) = 1$ implies $\gcd(\mathfrak{P}, 2\delta) = 1$, we have $\mathfrak{P}^\nu \mid D' - D - \delta$ or $\mathfrak{P}^\nu \mid D' - D + \delta$. It now follows immediately from Lemma 2 (with $\mathfrak{A} = \mathfrak{P}^\nu$) and $D' + D \equiv rs - 3 \pmod{\mathfrak{P}^\nu}$ of (137) that (143) holds in the first alternative and (144) holds in the second alternative. Conversely, assume (143) or (144) holds (in fact assume (143) holds—the other case being similar). Then from Lemma 2 with $\mathfrak{A} = \mathfrak{P}^\nu$ we have (139I), where $A(n-1)$, $A(n)$, $A(n+1)$ are read mod $\mathfrak{P}^\nu$ (or mod $\mathfrak{P}^\nu \cap \mathbf{Z}$). Now (143) certainly implies

$$\alpha^{-n} \equiv \beta^{-1}, \quad \beta^{-n} \equiv \gamma^{-1}, \quad \gamma^{-n} \equiv \alpha^{-1} \pmod{\mathfrak{P}^\nu},$$

and so, applying Lemma 2 to the reverse sequence (which simply interchanges r and s), we see

$$A(-n-1) \equiv r, \quad A(-n) \equiv s, \quad A(-n+1) \equiv D' \pmod{\mathfrak{P}^\nu},$$

where

$$D' \equiv \tfrac{1}{2}(rs - 3 - \delta') \pmod{\mathfrak{P}^\nu} \quad \text{and} \quad \delta' = (\alpha^{-1} - \beta^{-1})(\beta^{-1} - \gamma^{-1})(\gamma^{-1} - \alpha^{-1}).$$

But $\alpha\beta\gamma = 1$ implies $\delta' = -\delta$. We now solve the equations for D and D' to obtain (137) mod $\mathfrak{P}^\nu$. These equations do not depend on the choice (143) or (144) and thus hold for all prime ideals $\mathfrak{P} \mid m$. They then hold mod mI_K and so also mod m since $mI_K \cap \mathbf{Z} = m\mathbf{Z}$. □

We note that Lemma 2 and Theorem 3 say that the left half of the signature adds no new information. It is nevertheless important and convenient since it is automatically computed in the algorithm given in Section 5 and it makes the signature easier to recognize. That is, in the Q signature the two middle terms are the same, and in

the I signature the sum and difference of the two middle terms are easily recognizable. A propos of this point we have from the proof of Theorem 3:

COROLLARY 4. *Assume that* $\gcd(2d, m) = \gcd(r, s, m) = 1$ *and n has a Q signature* mod m. *Then the special rational integer root a in* (135) *may be obtained from the congruences*

$$(145) \qquad \begin{cases} (r^2 - 3s)a \equiv 3B - 2rs + rC & (\text{mod } m), \\ (s^2 - 3r)a \equiv -sB - rA + r(s^2 - r) & (\text{mod } m). \end{cases}$$

Finally, we prove that S, Q, and I signatures cannot be confused. More precisely:

PROPOSITION 5. *Assume that* n, m *are integers such that* $\gcd(2d, m) = 1$. *If n has a Q signature* mod m, *then*

$$(146) \qquad B \not\equiv 3 \ (\text{mod } m).$$

If n has an I signature mod m, *then*

$$(147) \qquad D \not\equiv D' \ (\text{mod } m).$$

Proof. Of course (147) is trivial since from (137) we have $(D' - D)^2 \equiv d \ (\text{mod } m)$. To prove (146) we assume, to the contrary, that $B \equiv 3 \ (\text{mod } m)$ and obtain from (138a) that

$$r^2s^2 + 18rs - 4(r^3 + s^3) - 27 \equiv 0 \ (\text{mod } m).$$

But the left side is the discriminant d of (129), and therefore $\gcd(2d, m) > 1$ if $m > 1$. □

14. The Signature of a Prime. In this section we apply the theory of the previous section to show that all primes have either an S, Q, or I signature. We recall that for any integer n, the signature of n mod n is called the *signature of n*.

Let p be a prime integer. We recall from Section 2 that p is called an S *prime* if $f(X) = X^3 - rX^2 + sX - 1$ splits into three linear factors mod p. It is called a Q *prime* if $f(X)$ splits into the product of a linear and irreducible quadratic polynomial mod p. Finally, it is called an I *prime* provided $f(X)$ is irreducible mod p.

THEOREM 6. *Assume p is a prime integer such that* $p \nmid 2d$. *Then p is an S, Q, I prime respectively if, and only if, p has an S, Q, I signature, respectively.*

Proof. Recall that $K = \mathbf{Q}(\alpha, \beta, \gamma)$ is the splitting field of $f(X)$. Set $F = \mathbf{Q}(\alpha)$. If $f(X)$ is reducible over $\mathbf{Q}$, the result is deducible in precisely the same way as given below (with $K = F$ a quadratic extension of $\mathbf{Q}$); we therefore assume $f(X)$ is irreducible over $\mathbf{Q}$. Then p is an S, Q, I prime mod p if, and only if, p splits in F as

S: product of three degree 1 primes,

Q: product of one degree 1 and one degree 2 prime,

I: p remains prime and has degree 3.

(p is unramified since we assumed $p \nmid d$.)

Assume that in K, p splits into a product of g primes of degree $\mathfrak{f}$. Then the above statement is equivalent to

$$S\colon \mathfrak{f} = 1 \quad \text{and} \quad \begin{cases} g = 6 & \text{if } K \neq F, \\ g = 3 & \text{if } K = F, \end{cases}$$

$$Q\colon \mathfrak{f} = 2 \quad \text{and} \quad g = 3 \quad (\text{here } K = F \text{ is impossible}),$$

$$I\colon \mathfrak{f} = 3 \quad \text{and} \quad \begin{cases} g = 2 & \text{if } K \neq F, \\ g = 1 & \text{if } K = F. \end{cases}$$

Now assume p is an S, Q, I prime, respectively, and $\mathfrak{P}$ is a prime of K lying over p. Then $I_K/\mathfrak{P}$ is a cyclic Galois extension of $\mathbf{Z}/p\mathbf{Z}$ of degree $\mathfrak{f}$ with generator of the Galois group given by $\rho \mapsto \rho^p \pmod{\mathfrak{P}}$. If p is an S prime, $\rho \mapsto \rho^p \pmod{\mathfrak{P}}$ is the identity map, and we see that $\alpha^p \equiv \alpha$, $\beta^p \equiv \beta$, $\gamma^p \equiv \gamma \pmod{\mathfrak{P}}$. If p is a Q prime, then one root of $f(X)$, say α, has the property that $\alpha \equiv a \pmod{\mathfrak{P}}$ with $a \in \mathbf{Z}$, and β generates the quadratic $I_K/\mathfrak{P}$ over $\mathbf{Z}/p\mathbf{Z}$; thus $\alpha^p \equiv \alpha \pmod{\mathfrak{P}}$, $\beta^p \equiv \gamma \pmod{\mathfrak{P}}$ (β^p is a conjugate of β mod $\mathfrak{P}$) and $\gamma^p \equiv \beta \pmod{\mathfrak{P}}$. If p is an I prime, then α^p is another root, say β, so $\alpha^p \equiv \beta \pmod{\mathfrak{P}}$, and α^{p^2} is another root ($\mathfrak{f} = 3$) so $\alpha^{p^2} \equiv \gamma \pmod{\mathfrak{P}}$; thus $\alpha^p \equiv \beta$, $\beta^p \equiv \gamma$, $\gamma^p \equiv \alpha \pmod{\mathfrak{P}}$. Then by Theorem 3 we see easily that p has the desired signature.

Conversely, assuming p has an S, Q, or I signature, we see by Theorem 3 that for all prime ideals $\mathfrak{P}$ lying over p in K the congruences of Theorem 3 hold. This implies degree $\mathfrak{P} = 1, 2$, or 3, respectively, and $\mathfrak{P}$ is of the desired type. □

Suppose K has degree 6 over $\mathbf{Q}$. Then the Galois group of $K/\mathbf{Q}$ is S_3, and in particular σ defined by $\alpha \mapsto \beta$, $\beta \mapsto \alpha$, $\gamma \mapsto \gamma$ is in the Galois group of $K/\mathbf{Q}$. Let $\mathfrak{P}$ be a prime ideal lying over the I prime p. Then by Theorem 6 we may assume the congruences (143) hold with $n = p$. Now $\sigma\mathfrak{P}$ is the other prime lying over p. Applying σ to the congruences (143), we see we obtain the congruences (144) mod $\sigma\mathfrak{P}$. Thus neither (143) nor (144) hold mod the ideal pI_K. This accounts for the necessity of including the two alternatives in the statement of Theorem 3 for I signatures. A similar comment, of course, applies for Q signatures.

15. The Period of the Recurrence. Since there are only a finite number of possible triples $(A(n-1), A(n), A(n+1)) \bmod m$, for some fixed integer m, the sequence $A(n)$ must be periodic mod m. We recall the notation that $W = W(m)$ denotes the period of $A(n)$ mod m.

THEOREM 7. *Let m be any integer such that* $\gcd(m, 2d) = 1$. *Then $W(m)$ is the least integer w such that*

$$\alpha^w \equiv \beta^w \equiv \gamma^w \equiv 1 \pmod{mI_K}. \tag{148}$$

For any such w in (148) *we have $W(m) \mid w$. Finally we have*

$$\begin{cases} W(m) \mid n-1 & \text{if } n \text{ has an } S \text{ signature} \bmod m, \\ W(m) \mid n^2-1 & \text{if } n \text{ has a } Q \text{ signature} \bmod m, \\ W(m) \mid n^2+n+1 & \text{if } n \text{ has an } I \text{ signature} \bmod m. \end{cases} \tag{149}$$

Proof. Since $A(k)$ satisfies the recurrence (127) for all integers k, both positive and negative, the sequence must be pure periodic. Thus we see that $W(m)$ may be

characterized as the least integer w such that $w+1$ has an S signature mod m. The first assertion now follows from Theorem 3. The second assertion is proved as usual, and it remains to prove (149). We apply Theorem 3. If n has an S signature mod m, then (141) implies $\alpha^{n-1} \equiv \beta^{n-1} \equiv \gamma^{n-1} \equiv 1 \pmod{mI_K}$ and so $W(m) \mid n-1$. If n has a Q signature mod m, then assuming, for example, the first alternative in (142) we have $\alpha^{n-1} \equiv 1 \pmod{\mathfrak{P}^\nu}$ so $\alpha^{n^2-1} \equiv 1 \pmod{\mathfrak{P}^\nu}$ and $\beta^{n^2-1} \equiv \gamma^n\beta^{-1} \equiv \beta\beta^{-1} \equiv 1 \pmod{\mathfrak{P}^\nu}$ and similarly $\gamma^{n^2-1} \equiv 1 \pmod{\mathfrak{P}^\nu}$. Since this holds for all prime ideals $\mathfrak{P} \mid m$ it holds mod mI_K and so $W(m) \mid n^2-1$. If n has an I signature mod m, then from (143) or (144) we have

$$\alpha^{n^2+n+1} \equiv \alpha^{n^2}\alpha^n\alpha \equiv \gamma\beta\alpha = 1 \pmod{\mathfrak{P}^\nu}$$

and similarly $\gamma^{n^2+n+1} \equiv \beta^{n^2+n+1} \equiv 1 \pmod{\mathfrak{P}^\nu}$. This holds for all prime ideals $\mathfrak{P} \mid m$ and so hold mod mI_K. Thus $W(m) \mid n^2+n+1$. □

COROLLARY 8. *Let p be a prime such that $p \nmid 2d$. Then*

$$(150) \qquad \begin{cases} W(p) \mid p-1 & \text{if } p \text{ is an } S \text{ prime}, \\ W(p) \mid p^2-1 & \text{if } p \text{ is a } Q \text{ prime}, \\ W(p) \mid p^2+p+1 & \text{if } p \text{ is an } I \text{ prime}. \end{cases}$$

The period may be identified in terms of the roots of $f(X)$. For this purpose we denote, for any prime integer p and any ρ in I_K prime to p, $\operatorname{ord}_p \rho$ the multiplicative order of ρ in I_K/pI_K.

COROLLARY 9. *Let p be a prime integer such that $p \nmid 2d$. Then*

(i) $W(p) = \operatorname{lcm}(\operatorname{ord}_p\alpha, \operatorname{ord}_p\beta, \operatorname{ord}_p\gamma)$ *if p is an S prime.*

(ii) $W(p) = \operatorname{ord}_p\beta = \operatorname{ord}_p\gamma$ *if p is a Q prime and α corresponds to the rational root of $f(X)$.*

(iii) $W(p) = \operatorname{ord}_p\alpha = \operatorname{ord}_p\beta = \operatorname{ord}_p\gamma$ *if p is an I prime.*

Proof. From Theorem 7 we always have

$$W(p) = \operatorname{lcm}(\operatorname{ord}_p\alpha, \operatorname{ord}_p\beta, \operatorname{ord}_p\gamma).$$

If p is a Q prime, we have from Corollary 8 that $\operatorname{ord}_p\beta, \operatorname{ord}_p\gamma \mid p^2-1$; then, since $\beta^p \equiv \gamma \pmod{pI_K}$ (from Theorem 3), we see that $\operatorname{ord}_p\beta = \operatorname{ord}_p\gamma$. Moreover

$$\alpha^{\operatorname{ord}_p\beta} = (\beta\gamma)^{-\operatorname{ord}_p\beta} \equiv 1 \pmod{pI_K},$$

and (ii) is established. Finally if p is an I prime, then Corollary 8 implies $\operatorname{ord}_p\alpha, \operatorname{ord}_p\beta, \operatorname{ord}_p\gamma \mid p^2+p+1$. It is then easily deduced from Theorem 3 that $\operatorname{ord}_p\alpha = \operatorname{ord}_p\beta = \operatorname{ord}_p\gamma$. □

We now prove the result that was used in the sieving in Section 4; i.e., Eq. (76):

PROPOSITION 10. *Let p be an I or Q prime such that $p \nmid 2d$. Let n be an integer such that $p \mid n$. Then*

$$(151) \qquad A(n) \equiv A(1) \quad \text{and} \quad A(-n) \equiv A(-1) \pmod{p}$$

holds if, and only if,

$$(152) \qquad n \equiv p^j \pmod{pW(p)}.$$

Here $j = 1$ or 2 if p is a Q prime, and $j = 1, 2, 3$ if p is an I prime.

Proof. That (152) implies (151) follows immediately from (132) and the definition of $W(p)$. Conversely assume (151). Write $n = mp$. From (132) we have $A(m) \equiv A(1)$ and $A(-m) \equiv A(-1) \pmod{p}$. From this and (131) we see that as polynomials

$$(153) \quad (X - \alpha^m)(X - \beta^m)(X - \gamma^m) \equiv (X - \alpha)(X - \beta)(X - \gamma) \pmod{pI_K}.$$

Let $\mathfrak{P}$ be any prime of K lying over p. Then (153) holds mod $\mathfrak{P}$ as well. Since $I_K/\mathfrak{P}$ is a field, we see that α, β, γ is some permutation of $\alpha^m, \beta^m, \gamma^m \bmod \mathfrak{P}$.

We first consider the case where p is an I prime. Say

$$(154) \qquad \alpha^p \equiv \beta, \quad \beta^p \equiv \gamma, \quad \gamma^p \equiv \alpha \pmod{\mathfrak{P}}.$$

Since $\alpha^m \equiv \alpha, \beta$ or $\gamma \pmod{\mathfrak{P}}$, we obtain

$$\alpha^m \equiv \alpha \quad \text{or} \quad \alpha^m \equiv \alpha^p \quad \text{or} \quad \alpha^m \equiv \alpha^{p^2} \pmod{\mathfrak{P}},$$

so that

$$(155) \qquad \alpha^{m-1} \equiv 1 \quad \text{or} \quad \alpha^{m-p} \equiv 1 \quad \text{or} \quad \alpha^{m-p^2} \equiv 1 \pmod{\mathfrak{P}}.$$

Then (154) implies that whichever alternative holds for α in (155) holds equally well for β and γ. From Theorem 7 we see that

$$W(p) \mid m - 1 \quad \text{or} \quad W(p) \mid m - p \quad \text{or} \quad W(p) \mid m - p^2,$$

as desired.

Now assume p is a Q prime and α is the rational root of $f(X) \bmod p$. Thus

$$\alpha^p \equiv \alpha, \quad \beta^p \equiv \gamma, \quad \gamma^p \equiv \beta \pmod{\mathfrak{P}}.$$

Again $\alpha^m \equiv \alpha, \beta$ or $\gamma \pmod{\mathfrak{P}}$. But $\alpha^m \equiv \beta \pmod{\mathfrak{P}}$ implies

$$\beta \equiv \alpha^m \equiv \alpha^{pm} \equiv \beta^p \equiv \gamma \pmod{\mathfrak{P}},$$

which contradicts the assumption that $p \nmid d$. Similarly $\alpha^m \not\equiv \gamma \pmod{\mathfrak{P}}$, and so $\alpha^m \equiv \alpha \pmod{\mathfrak{P}}$. Hence $\beta^m \equiv \beta$ or $\beta^m \equiv \gamma \equiv \beta^p \pmod{\mathfrak{P}}$ or $\beta^{m-1} \equiv 1$ or $\beta^{m-p} \equiv 1 \pmod{\mathfrak{P}}$. Thus, also $\gamma^{m-1} \equiv 1$ or $\gamma^{m-p} \equiv 1 \pmod{\mathfrak{P}}$, respectively. Since we also have

$$\alpha^{m-1} \equiv \alpha^{m-p} \equiv 1 \pmod{\mathfrak{P}},$$

we see in fact that $W(p) \mid m - 1$ or $W(p) \mid m - p$. □

We recall that Proposition 10 may be false when p is an S prime. In Section 4 we gave an example of an $A(n)$ where the S prime 29 had $m = 9$ as an outsider.

16. Constructing Composites with Interesting Signatures. We begin with the following observation.

PROPOSITION 11. *Let n be an integer such that* $\gcd(n, 2d) = 1$. *Let $p \mid n$ be a prime. Assume n has an S signature. If p is an S, Q, or I prime, respectively, then $n \equiv p, p^2$, or $p^3 \pmod{pW(p)}$, respectively. Conversely, if $n \equiv p \pmod{pW(p)}$, then p is an S prime; if $n \equiv p^2 \pmod{pW(p)}$, then p is an S or Q prime; if $n \equiv p^3 \pmod{pW(p)}$, then p is an S or I prime.*

Proof. Since n has an S signature mod n, we see that n has an S signature mod p as well. Thus from Theorem 7 we see that $W(p) \mid n - 1$. If p is an S prime, then $W(p) \mid p - 1$ (Corollary 8), and so $W(p) \mid n - p = n - 1 - (p - 1)$; since

$\gcd(p, p-1) = 1$, we see in fact that $n \equiv p \pmod{pW(p)}$. Conversely assume $n \equiv p \pmod{pW(p)}$. Then $W(p) \mid p - 1 = n - 1 - (n - p)$, and so $\alpha^{p-1} \equiv \beta^{p-1} \equiv \gamma^{p-1} \equiv 1 \pmod{pI_K}$, and so p is an S prime.

If p is a Q prime, we have from Proposition 10 that $n \equiv p, p^2 \pmod{pW(p)}$. If $n \equiv p \pmod{pW(p)}$, we see that n has a Q signature mod p which cannot be, by Proposition 5 (since p has a Q signature mod p and $A(\pm n + j) \equiv A(\pm p + j) \pmod{p}$). Conversely if $n \equiv p^2 \pmod{pW(p)}$, we see that $W(p) \mid p^2 - 1$. If p were an I prime, then $W(p) \mid p^2 + p + 1$ and so $W(p) \mid 3$. If $W(p) = 3$, then $3 \mid p - 1$ (since $3 = \gcd(p^2 - 1, p^2 + p + 1)$), and we have $W(p) \mid p - 1$ so p has an S signature, contradicting the assumption that p has an I signature.

Finally, suppose p is an I prime. Then from Proposition 10 we have that $n \equiv p, p^2, p^3 \pmod{pW(p)}$. Let $\mathfrak{P}$ be a prime of K lying over p. Since p is an I prime, we may assume $\alpha^p \equiv \beta$, $\beta^p \equiv \gamma$, $\gamma^p \equiv \alpha \pmod{\mathfrak{P}}$. Then if $n \equiv p \pmod{pW(p)}$, we see $\alpha^n \equiv \beta$, $\beta^n \equiv \gamma$, $\gamma^n \equiv \alpha \pmod{\mathfrak{P}}$, and n has an I signature mod $\mathfrak{P}$, which it does not. If $n \equiv p^2 \pmod{pW(p)}$, then

$$\alpha^n \equiv \alpha^{p^2} \equiv \beta^p \equiv \gamma \pmod{\mathfrak{P}},$$

and similarly $\gamma^n \equiv \beta$, $\beta^n \equiv \alpha \pmod{\mathfrak{P}}$, and again n has an I signature, which it does not. Thus $n \equiv p^3 \pmod{pW(p)}$. If $n \equiv p^3 \pmod{pW(p)}$ and p has a Q signature, then $W(p) \mid p^2 - 1$ and $W(p) \mid n - 1$ implies $W(p) \mid p - 1 = \gcd(p^2 - 1, p^3 - 1)$, and so p is an S prime which is a contradiction. So we see p is an S or I prime. □

COROLLARY 12. *If n is a square free product of S primes, then n has an S signature if, and only if, for all primes $p \mid n$, $n/p \equiv 1 \pmod{W(p)}$.*

Proof. If n has an S signature, then $n/p \equiv 1 \pmod{W(p)}$ follows from Proposition 11. Conversely, since p is an S prime, we see

$$\alpha^n \equiv \alpha^{pn/p} \equiv \alpha^{n/p} \equiv \alpha \pmod{pI_K},$$

and similarly $\beta^n \equiv \beta$, $\gamma^n \equiv \gamma \pmod{pI_K}$. Thus n has an S signature mod p for all $p \mid n$. Since n is square free, we see n has an S signature. □

All of the examples of composites with S signatures were examples of this phenomenon. For example, if n is a Carmichael number, then for all prime integers

$$p \mid n \quad \text{implies} \quad p - 1 \mid n - 1. \tag{156}$$

If p is an S prime and $p \mid n$, then $W(p) \mid p - 1$, and so $n/p \equiv 1 \pmod{W(p)}$. So Carmichael numbers made up of S primes automatically yield composites with S signatures. Similarly the O_i of Section 7 were composites $n = p(2p - 1)$ where p, $2p - 1$ were both S primes and $W(2p - 1) \mid p - 1$. We see that these conditions simply insured that $n/p \equiv 1 \pmod{W(2p - 1)}$ and $n/(2p - 1) \equiv 1 \pmod{W(p)}$.

Corresponding to Proposition 11 we have

PROPOSITION 13. *Let n be an integer such that $\gcd(n, 2d) = 1$. Let p be a prime, $p \mid n$.*

(i) *If n has a Q signature, then p is an S or Q prime, and if p is a Q prime, then $n \equiv p \pmod{pW(p)}$.*

(ii) *If n has an I signature, then p is an S or I prime, and if p is an I prime, then $n \equiv p, p^2 \pmod{pW(p)}$.*

Proof. If n has a Q signature, there is a rational integer a such that $f(a) \equiv 0 \pmod{n}$, and so $f(a) \equiv 0 \pmod{p}$. Thus p cannot be an I prime. Moreover if p is a Q prime, we have from Proposition 10, $n \equiv p$ or $p^2 \pmod{pW(p)}$. If $n \equiv p^2 \pmod{pW(p)}$, we see that p would have an S signature mod p contrary to our assumption.

Similarly if n has an I signature, then $(D' - D)^2 \equiv d \pmod{n}$, and so $(D' - D)^2 \equiv d \pmod{p}$, and we see that p cannot be a Q prime. Again we are done by Proposition 10 since $n \equiv p^3 \pmod{pW(p)}$ for an I prime p implies n has an S signature mod p. □

If we do not restrict ourselves to a particular sequence (like Perrin), but instead allow any sequence, it is easy to construct composites made up of S primes with S or Q or I signatures. For example, let n be any Carmichael number. Then (156) holds for all primes $p \mid n$, and so for all integers a, b, c prime to n we have $a^{n-1} \equiv b^{n-1} \equiv c^{n-1} \equiv 1 \pmod{n}$. Choose a, b, c so that $abc \equiv 1 \pmod{n}$. Set

$$f(X) \equiv (X - a)(X - b)(X - c) \equiv X^3 - rX^2 + sX - 1 \pmod{n}. \tag{157}$$

For the infinite class of irreducible cubic equations contained in (157) we have that n has an S signature and for each prime $p \mid n$, p is an S prime.

Instead of considering (156) we could consider square free integers n such that for all primes p

$$p \mid n \quad \text{implies} \quad p - 1 \mid n^2 - 1. \tag{158}$$

Assume we have an integer b prime to n such that $b^{n-1} \not\equiv 1 \pmod{n}$ (so we are assuming (156) does not hold). Set $c \equiv b^n \pmod{n}$. Then $c^n \equiv b^{n^2} \equiv b \pmod{n}$ (since $b^{n^2-1} \equiv 1 \pmod{p}$ for all primes $p \mid n$). Define a by $abc \equiv 1 \pmod{n}$. Then $a^n \equiv (bc)^{-n} \equiv (b^n c^n)^{-1} \equiv (cb)^{-1} \equiv a \pmod{n}$. Again define the recurrence by (157), and we see that we obtain a composite integer n with a Q signature such that for each prime $p \mid n$ we have p as an S prime. Here, of course, $(d/p) = 1$ for all $p \mid n$, and so $(d/n) = 1$ as well, and we see n does not have an acceptable Q signature. An example of this phenomenon is given by $n = 35$ and is discussed in Section 8 (see (98), (99)).

Instead of either (156) or (158) we may consider composites n such that for all primes p

$$p \mid n \quad \text{implies} \quad p - 1 \mid n^3 - 1. \tag{159}$$

Then let a be any integer prime to n so that $a^{n-1} \not\equiv 1 \pmod{n}$ and $a^{n^2-1} \not\equiv 1 \pmod{n}$ and $a^{n^2-n} \not\equiv 1 \pmod{n}$ but $a^{n^2+n+1} \equiv 1 \pmod{n}$. It is not hard to find such an a because of the assumption (159) on n. Set $b \equiv a^n \pmod{n}$ and $c \equiv b^n \pmod{n}$. This time (157) defines a recurrence where n has an I signature and each prime $p \mid n$ is an S prime. As noted in Section 8, however, these I composites never have an acceptable I signature as they are caught by the form test. An example of this phenomenon is given in Section 8 (see (100)) with $n = 1537$ and $a = 36$.

17. The Recurrence Mod Prime Powers. We finally prove a congruence that was needed in Sections 1 and 4.

THEOREM 14. *Let p be any prime. Then for all integers $k \geq 1$*

$$A(p^k) \equiv A(p^{k-1}) \pmod{p^k}. \tag{160}$$

COROLLARY 15. *Let p be any prime and m be any integer. Then for all integers $k \geq 1$*

$$A(mp^k) \equiv A(mp^{k-1}) \pmod{p^k}.$$

We require the following

LEMMA 16. *There is a polynomial $h(X, Y)$ with integer coefficients of degree $\leq p-1$, depending only on p, such that for all m*

$$A(mp) = A(m)^p + ph(A(m), A(-m)). \tag{161}$$

Proof. As in the derivation of (132) we may assume $m = 1$ and expand $A(1)^p$ to obtain

$$A(1)^p = A(p) + pH(\alpha, \beta, \gamma), \tag{162}$$

where $H(X, Y, Z)$ is a *symmetric* polynomial of degree $\leq p-1$. Setting $\sigma_1(X, Y, Z) = X + Y + Z$, $\sigma_2(X, Y, Z) = XY + YZ + ZX$, $\sigma_3(X, Y, Z) = XYZ$, we have $H(X, Y, Z) = G(\sigma_1, \sigma_2, \sigma_3)$. Noting that $\sigma_1(\alpha, \beta, \gamma) = A(1)$, $\sigma_2(\alpha, \beta, \gamma) = A(-1)$ and $\sigma_3(\alpha, \beta, \gamma) = 1$, we see that (162) immediately implies (161). The condition on the degree of h follows from the theory of symmetric functions. □

Equation (161) for $m = \pm p^{k-1}$ gives

$$A(p^k) = A(p^{k-1})^p + ph(A(p^{k-1}), A(-p^{k-1})), \tag{163}$$

$$A(-p^k) = A(-p^{k-1})^p + ph(A(-p^{k-1}), A(p^{k-1})). \tag{164}$$

To prove (160) we prove by induction on $k \geq 1$ the equation (160) and also

$$A(-p^k) \equiv A(-p^{k-1}) \pmod{p^k}. \tag{165}$$

For $k = 1$ we simply apply (163) and (164) with $k = 1$, noting that $A(1)^p \equiv A(1)$, $A(-1)^p \equiv A(-1) \pmod{p}$. By induction we assume (160) and (165) with k replaced by $k-1$. Then we also obtain

$$ph(A(p^{k-1}), A(-p^{k-1})) \equiv ph(A(p^{k-2}), A(-p^{k-2})) \pmod{p^k}. \tag{166}$$

Since in general $u \equiv v \pmod{p^{k-1}}$ implies $u^p \equiv v^p \pmod{p^k}$, we also obtain

$$A(p^{k-1})^p \equiv A(p^{k-2})^p \pmod{p^k}. \tag{167}$$

Thus from (163), (166), and (167) we see

$$\begin{aligned} A(p^k) &= A(p^{k-1})^p + ph(A(p^{k-1}), A(-p^{k-1})) \\ &\equiv A(p^{k-2})^p + ph(A(p^{k-2}), A(-p^{k-2})) \pmod{p^k} \\ &= A(p^{k-1}). \end{aligned}$$

This gives (160). Equation (165) is proved similarly. □

We note that it follows immediately from (160) that in the p-adic integers $\mathbf{Z}_p$ that $\lim_{k\to\infty} A(p^k)$ exists. Set

$$A_\cdot = \lim_{k\to\infty} A(\pm p^k).$$

It follows immediately from (163) and (164) that

$$A_+ = A_+^p + ph(A_+, A_-), \quad A_- = A_-^p + ph(A_-, A_+).$$

For example, if $p = 2$, we see that (163) is just the doubling rule (55), and we obtain

$$A_+ = A_+^2 - 2A_-, \quad A_- = A_-^2 - 2A_+,$$

which can be solved to yield

$$A_+(A_+ - 3)(A_+^2 + A_+ + 2) = 0.$$

Indeed we can easily show

$$\lim_{k\to\infty} A(2^k) = \begin{cases} 3 & \text{if } r \equiv s \equiv 1 \pmod 2, \\ 0 & \text{if } r \equiv s \equiv 0 \pmod 2, \\ \dfrac{-1+\sqrt{-7}}{2} & \text{if } r + s \equiv 1 \pmod 2. \end{cases} \tag{168}$$

Equation (168) is proved by proving the following congruences by induction on k. In the case where $r \equiv s \equiv 1 \pmod 2$ (which is equivalent to the statement $2 \mid d$) we show that for all $k \geqslant 0$

$$A(2^k) \equiv A(-2^k) \equiv 3 \pmod{2^k}.$$

When $r \equiv s \equiv 0 \pmod 2$ we show that for all $k \geqslant 0$

$$A(2^k) \equiv A(-2^k) \equiv 0 \pmod{2^k}.$$

Finally when $r + s \equiv 1 \pmod 2$ (one of r, s is even and the other odd) we show that

$$A(2^k) + A(-2^k) \equiv -1 \pmod{2^k}, \quad A(2^k)A(-2^k) \equiv 2 \pmod{2^k}.$$

Our forthcoming paper [12] begins where we stop here and evaluates $A_{r,s}$ for all p and all r and s. They are Abelian algebraic integers. We then examine their implications for the earlier theory given above.

In particular, we can now construct *acceptable* Q and I composites, (satisfying the Jacobi Symbol and F-tests), for certain cubics (39). Some of them contain no S-prime divisor, and so no outsiders are needed for that type of acceptable composite. But we still have no acceptable Q or I composite for the -23, -31, or -44 $A(n)$, either with or without S-prime divisors. They probably are very sparse if they do exist. One reason is this: If n is one of these constructed acceptable composites, the discriminant of its cubic is $O(n^4)$. The probability that such a cubic has a discriminant equal to -23, -31, or -44 is therefore very small. There are other cogent reasons [12] why -23, etc. are so hard to obtain in these constructions, and it could be that they do not exist.

A modest example of these new constructions is $n = 87 = 3 \cdot 29$ in $x^3 - 26x^2 + 12x - 1$ with $d = +25717$ (only). The class number of the real field $Q(\sqrt{d})$ is 3. Here, 3 and 29 are I primes, and n has an acceptable I signature 26, 12, 43, 5, 26, 12 and an (indefinite) I form $F = (87, 49, -67)$. In [12] we give the p-adic techniques for constructing such examples.

18. Acknowledgements. We mentioned S. Haber in Section 1. Later he told us that he also told Morris Newman about the problem who, independently, found $n = 521^2$ and an $O(\log n)$ algorithm. We do not know the details but have some reason to think that Newman's treatment differed from ours in both of these items. We would like to thank J. Owings for the idea for constructing the examples in Section 7, for

his interest and useful comments and for procuring some hard to find references. Finally, we wish to thank H. W. Lenstra and the Lehmers for their interest during the course of this investigation.

Appendix I

Perrin Primes

The following table lists the first 120 primes in column 1. In column 2 is listed the type of prime in the Perrin field of discriminant -23 for $f(X) = X^3 - X - 1$. Here, as usual, S denotes a split prime, Q denotes a 1–2 prime and I denotes an inert prime. The fractional notation in column 2 denotes the fraction of the full possible period. That is, the notation $S/2$ means the S prime has period $W = (p-1)/2$, $Q/3$ means the Q prime has period $W = (p^2-1)/3$ and $I/21$ means the I prime has period $(p^2+p+1)/21$. Finally, the third column gives the factorization of the period W (where we place a p if W itself is prime).

p	type	W factored	p	type	W factored
2	I	p	179	I	$7 \cdot 4603$
3	I	p	181	$Q/3$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13$
5	Q	$2^3 \cdot 3$	191	$Q/5$	$2^7 \cdot 3 \cdot 19$
7	Q	$2^4 \cdot 3$	193	I	$3 \cdot 7 \cdot 1783$
11	Q	$2^3 \cdot 3 \cdot 5$	197	I	$19 \cdot 2053$
13	I	$3 \cdot 61$	199	Q	$2^4 \cdot 3^2 \cdot 5^2 \cdot 11$
17	Q	$2^5 \cdot 3^2$	211	S	$2 \cdot 3 \cdot 5 \cdot 7$
19	$Q/2$	$2^2 \cdot 3^2 \cdot 5$	223	$S/2$	$3 \cdot 37$
23	R	$2 \cdot 11$	227	Q	$2^3 \cdot 3 \cdot 19 \cdot 113$
29	I	$13 \cdot 67$	229	$Q/24$	$5 \cdot 19 \cdot 23$
31	I	$3 \cdot 331$	233	I	$7 \cdot 7789$
37	Q	$2^3 \cdot 3^2 \cdot 19$	239	I	$19 \cdot 3019$
41	I	p	241	Q	$2^5 \cdot 3 \cdot 5 \cdot 11^2$
43	$Q/8$	$3 \cdot 7 \cdot 11$	251	Q	$2^3 \cdot 3^2 \cdot 5^3 \cdot 7$
47	I	$37 \cdot 61$	257	I	$61 \cdot 1087$
53	$Q/2$	$2^2 \cdot 3^3 \cdot 13$	263	$Q/2$	$2^3 \cdot 3 \cdot 11 \cdot 131$
59	S	$2 \cdot 29$	269	I	$13 \cdot 37 \cdot 151$
61	$Q/4$	$2 \cdot 3 \cdot 5 \cdot 31$	271	S	$2 \cdot 3^3 \cdot 5$
67	Q	$2^3 \cdot 3 \cdot 11 \cdot 17$	277	I	$7 \cdot 19 \cdot 579$
71	I	p	281	$Q/7$	$2^4 \cdot 3 \cdot 5 \cdot 47$
73	I	$3 \cdot 1801$	283	Q	$2^3 \cdot 3 \cdot 47 \cdot 71$
79	$Q/2$	$2^4 \cdot 3 \cdot 5 \cdot 13$	293	$Q/14$	$2^2 \cdot 3 \cdot 7 \cdot 73$
83	$Q/3$	$2^3 \cdot 7 \cdot 41$	307	S	$2 \cdot 3^2 \cdot 17$
89	$Q/2$	$2^3 \cdot 3^2 \cdot 5 \cdot 11$	311	I	$19 \cdot 5107$
97	$Q/3$	$2^6 \cdot 7^2$	313	$Q/6$	$2^3 \cdot 13 \cdot 157$
101	S	$2^2 \cdot 5^2$	317	S	$2^2 \cdot 79$
103	$Q/3$	$2^4 \cdot 13 \cdot 17$	331	I	$3 \cdot 7 \cdot 5233$
107	$Q/4$	$2 \cdot 3^3 \cdot 53$	337	$Q/6$	$2^4 \cdot 7 \cdot 13^2$
109	$Q/8$	$3^3 \cdot 5 \cdot 11$	347	$S/2$	p
113	$Q/3$	$2^5 \cdot 7 \cdot 19$	349	I	$3 \cdot 19 \cdot 2143$
127	I	$3 \cdot 5419$	353	I	$19 \cdot 6577$
131	I	p	359	$Q/10$	$2^3 \cdot 3^2 \cdot 179$
137	$Q/48$	$17 \cdot 23$	367	Q	$2^5 \cdot 3 \cdot 23 \cdot 61$
139	I	$3 \cdot 13 \cdot 499$	373	Q	$2^3 \cdot 3 \cdot 11 \cdot 17 \cdot 31$
149	$Q/24$	$5^2 \cdot 37$	379	$Q/2$	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 19$
151	$I/21$	p	383	$Q/8$	$2^5 \cdot 3 \cdot 191$
157	$Q/2$	$2^2 \cdot 3 \cdot 13 \cdot 79$	389	$Q/2$	$2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 97$
163	$I/3$	$7 \cdot 19 \cdot 67$	397	$I/3$	$31 \cdot 1699$
167	S	$2 \cdot 83$	401	Q	$2^5 \cdot 3 \cdot 5^2 \cdot 67$
173	S	$2^2 \cdot 43$	409	$I/3$	p

p	type	W factored	p	type	W factored
419	$Q/2$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	547	$I/3$	$163 \cdot 613$
421	$Q/3$	$2^3 \cdot 5 \cdot 7 \cdot 211$	557	$Q/18$	$2^2 \cdot 31 \cdot 139$
431	$Q/2$	$2^4 \cdot 3^3 \cdot 5 \cdot 43$	563	$Q/8$	$3 \cdot 47 \cdot 281$
433	Q	$2^5 \cdot 3^3 \cdot 7 \cdot 31$	569	Q	$2^4 \cdot 3 \cdot 5 \cdot 19 \cdot 71$
439	I	$3 \cdot 31^2 \cdot 67$	571	Q	$2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19$
443	I	$7 \cdot 28099$	577	I	$3 \cdot 19 \cdot 5851$
449	$S/2$	$2^5 \cdot 7$	587	I	$547 \cdot 631$
457	Q	$2^4 \cdot 3 \cdot 19 \cdot 229$	593	S	$2^4 \cdot 37$
461	I	$373 \cdot 571$	599	S	$2 \cdot 13 \cdot 23$
463	$S/2$	$3 \cdot 7 \cdot 11$	601	$I/3$	$13 \cdot 9277$
467	$Q/18$	$2^2 \cdot 13 \cdot 233$	607	S	$2 \cdot 3 \cdot 101$
479	Q	$2^6 \cdot 3 \cdot 5 \cdot 239$	613	Q	$2^3 \cdot 3^2 \cdot 17 \cdot 307$
487	I	$3 \cdot 7 \cdot 11317$	617	$Q/6$	$2^3 \cdot 7 \cdot 11 \cdot 103$
491	I	$37 \cdot 6529$	619	$Q/6$	$2^2 \cdot 5 \cdot 31 \cdot 103$
499	I	$3 \cdot 7 \cdot 109^2$	631	$Q/6$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 79$
503	$Q/2$	$2^3 \cdot 3^2 \cdot 7 \cdot 251$	641	$Q/6$	$2^7 \cdot 5 \cdot 107$
509	I	$43 \cdot 6037$	643	Q	$2^3 \cdot 3 \cdot 7 \cdot 23 \cdot 107$
521	$Q/6$	$2^3 \cdot 3 \cdot 5 \cdot 13 \cdot 29$	647	I	$211 \cdot 1987$
523	$Q/3$	$2^3 \cdot 3 \cdot 29 \cdot 131$	653	I	$7 \cdot 13^2 \cdot 19^2$
541	$I/3$	$7 \cdot 13963$	659	Q	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 47$

Appendix 2

Perrin Signature Program

This is an HP-41C program for the Perrin signatures. For the signature of n (mod m) with n odd, place n, m in the stack and execute PS. If $m > 10^5$, it requires double precision and goes slower. Flag 2 is then set at instruction 4 and LBL 07 is used. If $m > 10^9$, there may be error, but n can be $< 10^{10}$. PS could be altered to

Perrin Signatures

```
LBL PS   3       XEQ 02   RCL 06   RCL 07   LAST X   MOD      RCL 11 END
1 E5     STO 03  STO 10   RCL 01   RCL 08   X↗2      13       STO 08
X ≤ Y?   0       RCL 02   XEQ 02   RCL 09   RCL 00   RCL 15   −
SF 02    2       RCL 05   STO 01   RCL 10   MOD      −        RCL 00
RDN      LBL 05  XEQ 02   +        FC?C 01  X <> Y    STO 15   MOD
STO 00   STO 06  STO 08   XEQ 04   RDN      RCL 00   RDN      STO 07
RDN      RDN     −        LBL 10   GTO 05   MOD      STOIND 15 +
STO 17   STO 05  XEQ 04   FS? 01   LBL 07   2        ISG 16   RCL 00
STO 13   RDN     STO 07   GTO 03   13       *        GTO 08   MOD
LN       STO 04  RCL 03   GTO 01   STO 15   +        STO 01   STO 09
2        RCL 13  RCL 04   LBL 02   .005     R↗       RCL 09   RCL 04
LN       X = 0?  XEQ 02   X↗2      STO 16   X↗2      RCL 08   GTO 10
/        GTO 06  +        X <> Y   LBL 08   RCL 00   STO 03   LBL 06
INT      RCL 14  XEQ 04   −        7        MOD      −        CF 02
2        X > Y?  STO 09   LAST X   ST − 15   +        RCL 00   RCL 01
X <> Y   GTO 00  RCL 04   −        RCLIND 15 7        MOD      STOP
Y↗X      ST − 13 RCL 03   LBL 04   ENTER    RCL 15   STO 02   RCL 02
ST − 13  SF 01   XEQ 02   RCL 00   ENTER    −        RCL 01   STOP
2        LBL 00  RCL 05   MOD      1 E5     STO 15   +        RCL 03
/        2       RCL 02   RTN      MOD      RDN      RCL 00   STOP
STO 14   ST/14   XEQ 02   LBL 01   −        RCLIND 15 MOD     RCL 04
1        FS? 02  STO 03   X <> 03  ENTER    −        STO 04   STOP
STO 01   GTO 07  −        X <> 02  ENTER    LAST X   RCL 10   RCL 05
CHS      RCL 01  XEQ 04   STO 01   LAST X   −        RCL 12   STOP
STO 02   RCL 06  STO 02   LBL 03   *        RCL 00   STO 10   RCL 06
```

accept n even, but in practice one does the signature of $n+1$ instead and extrapolates. The -31 sequence requires minor changes if $m < 10^5$. Likewise, the -44 for m odd and $< 10^5$ is possible with rather more changes. The signature, which is in memory 01 thru 06, is given at LBL 06. This computer interprets (mod 0) as "do nothing", so $m = 0$ gives Perrin's $A(n)$ unreduced if it does not overflow, i.e., if $n < 81$. This program has been very helpful during this investigation.

Department of Mathematics
University of Maryland
College Park, Maryland 20742

1. R. PERRIN, "Item 1484," *L'Intermédiare des Math.*, v. 6, 1899, pp. 76–77.

2. E. MALO, *ibid.*, v. 7, 1900, p. 281, p. 312.

2a. E. B. ESCOTT, *ibid.*, v. 8, 1901, pp. 63–64.

3. DOV JARDEN, *Recurring Sequences*, Riveon Lematematika, Jerusalem, 1966.

4. DANIEL SHANKS, "Calculation and applications of Epstein zeta functions," *Math. Comp.*, v. 29, 1975, pp. 271–287, esp. §8.

5. DANIEL SHANKS, "Five number-theoretic algorithms," *Proc. Second Manitoba Conf. on Numer. Math.*, 1972, pp. 51–70, esp. §§5 and 6.

6. DONALD ERVIN KNUTH, *Seminumerical Algorithms*, Second printing, Addison-Wesley, Reading, Mass., 1971, esp. pp. 260–266.

7. C. POMERANCE, J. L. SELFRIDGE & S. S. WAGSTAFF, Jr., "The pseudoprimes to $25 \cdot 10^9$," *Math. Comp.*, v. 35, 1980, pp. 1003–1026.

8. DANIEL SHANKS, "Review of Fröberg," *ibid.*, v. 29, 1975, pp. 331–333.

9. DANIEL SHANKS, "A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view)," *Proc. 7th SE Conf. on Combinatorics, Graph Theory, and Computing*, 1976, pp. 15–40, esp. p. 32 and [36], [45], [47], [48] cited there.

10. DANIEL SHANKS, "Class number, A theory of factorization, and genera," *Proc. Sympos. Pure Math.*, Vol. 20, 1971, pp. 415–440, esp. App. 1.

11. DANIEL SHANKS, *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 1978, esp. Sec. 69.

12. WILLIAM ADAMS & DANIEL SHANKS, "Strong primality tests. II—Algebraic identification of the p-adic limits and their implications." (To appear.)