2
How to Recognize Whether a Natural Number is a Prime

In the article 329 of *Disquisitiones Arithmeticae*, Gauss (1801) wrote:

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic.... The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

The first observation concerning the problem of primality and factorization is clear: there is an algorithm for both problems. By this, I mean a procedure involving finitely many steps, which is applicable to every number N and which will indicate whether N is a prime, or, if N is composite, which are its prime factors. Namely, given the natural number N, try in succession every number $n = 2, 3, \ldots$ up to $[\sqrt{N}]$ (the largest integer not greater than $\sqrt{N}$) to see whether it divides N. If none does, then N is a prime. If, say, N_0 divides N, write $N = N_0 N_1$, so $N_1 < N$, and then repeat the same procedure with N_0 and with N_1. Eventually this gives the complete factorization into prime factors.

What I have just said is so evident as to be irrelevant. It should, however, be noted that for large numbers N, it may take a long time with this algorithm to decide whether N is prime or composite.

This touches the most important practical aspect, the need to find an efficient algorithm—one which involves as few operations as possible, and therefore requires less time and costs less money to be performed.

It is my intention to divide this chapter into several sections in which I will examine various approaches, as well as explain the required theoretical results.

I   The Sieve of Eratosthenes

As I have already said, it is possible to find if N is a prime using trial division by every number n such that $n^2 \leq N$.

Since multiplication is an easier operation than division, Eratosthenes (in the 3rd century BC) had the idea of organizing the computations in the form of the well-known sieve. It serves to determine all the prime numbers, as well as the factorizations of composite numbers, up to any given number N. This is illustrated now for $N = 101$.

Do as follows: write all the numbers up to 101; cross out all the multiples of 2, bigger than 2; in each subsequent step, cross out all the multiples of the smallest remaining number p, which are bigger than p. It suffices to do it for $p^2 < 101$.

$$
\begin{array}{cccccccccc}
 & 2 & 3 & \cancel{4} & 5 & \cancel{6} & 7 & \cancel{8} & \cancel{9} & \cancel{10} \\
11 & \cancel{12} & 13 & \cancel{14} & \cancel{15} & \cancel{16} & 17 & \cancel{18} & 19 & \cancel{20} \\
\cancel{21} & \cancel{22} & 23 & \cancel{24} & \cancel{25} & \cancel{26} & \cancel{27} & \cancel{28} & 29 & \cancel{30} \\
31 & \cancel{32} & \cancel{33} & \cancel{34} & \cancel{35} & \cancel{36} & 37 & \cancel{38} & \cancel{39} & \cancel{40} \\
41 & \cancel{42} & 43 & \cancel{44} & \cancel{45} & \cancel{46} & 47 & \cancel{48} & \cancel{49} & \cancel{50} \\
\cancel{51} & \cancel{52} & 53 & \cancel{54} & \cancel{55} & \cancel{56} & \cancel{57} & \cancel{58} & 59 & \cancel{60} \\
61 & \cancel{62} & \cancel{63} & \cancel{64} & \cancel{65} & \cancel{66} & 67 & \cancel{68} & \cancel{69} & \cancel{70} \\
71 & \cancel{72} & 73 & \cancel{74} & \cancel{75} & \cancel{76} & \cancel{77} & \cancel{78} & 79 & \cancel{80} \\
\cancel{81} & \cancel{82} & 83 & \cancel{84} & \cancel{85} & \cancel{86} & \cancel{87} & \cancel{88} & 89 & \cancel{90} \\
\cancel{91} & \cancel{92} & \cancel{93} & \cancel{94} & \cancel{95} & \cancel{96} & 97 & \cancel{98} & \cancel{99} & \cancel{100} \\
101 & & & & & & & & &
\end{array}
$$

Thus, all the multiples of $2, 3, 5, 7 < \sqrt{101}$ are sifted away. The number 53 is prime because it remained. Thus the primes up to 101

are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101.

This procedure is the basis of sieve theory, which has been developed to provide estimates for the number of primes satisfying given conditions.

II   Some Fundamental Theorems on Congruences

In this section, I intend to describe some classical methods to test primality and to find factors. They rely on theorems on congruences, especially Fermat's little theorem, the old theorem of Wilson, as well as Euler's generalization of Fermat's theorem. I shall also include a subsection on quadratic residues, a topic of central importance, which is also related with primality testing, as I shall have occasion to indicate.

A   FERMAT'S LITTLE THEOREM AND PRIMITIVE ROOTS MODULO A PRIME

Fermat's Little Theorem. *If p is a prime number and if a is an integer, than $a^p \equiv a \pmod{p}$. In particular, if p does not divide a then $a^{p-1} \equiv 1 \pmod{p}$.*

Euler published the first proof of Fermat's little theorem.

Proof. It is true for $a = 1$. Assuming that it is true for a, then, by induction, $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$. So the theorem is true for every natural number a. $\square$

The above proof required only the fact that if p is a prime number and if $1 \le k \le p - 1$, then the binomial coefficient $\binom{p}{k}$ is a multiple of p.

Note the following immediate consequence: if $p \nmid a$ and p^n is the highest power of p dividing $a^{p-1} - 1$, then p^{n+e} is the highest power of p dividing $a^{p^e(p-1)} - 1$ (where $e \ge 1$); in this statement, if $p = 2$, then n must be at least 2.

It follows from the theorem that for any integer a, which is not a multiple of the prime p, there exists the smallest exponent $h \ge 1$, such that $a^h \equiv 1 \pmod{p}$. Moreover, $a^k \equiv 1 \pmod{p}$ if and only if h divides k; in particular, h divides $p-1$. This exponent h is called the

order of a modulo p. Note that $a \bmod p$, $a^2 \bmod p, \ldots , a^{h-1} \bmod p$, and $1 \bmod p$ are all distinct.

It is a basic fact that for every prime p there exists at least one integer g, not a multiple of p, such that the order of g modulo p is equal to $p-1$. Then, the set $\{1 \bmod p,\ 2 \bmod p, \ldots , g^{p-2} \bmod p\}$ is equal to the set $\{1 \bmod p,\ 2 \bmod p, \ldots , (p-1) \bmod p\}$.

Every integer g, $1 \leq g \leq p-1$, such that $g \bmod p$ has order $p-1$, is called a *primitive root modulo p.* I note this proposition:

Let p be any odd prime, $k \geq 1$, and $S = \sum_{j=1}^{p-1} j^k$. Then

$$S \equiv \begin{cases} -1 \bmod p, & \text{when } p-1 \mid k, \\ 0 \bmod p, & \text{when } p-1 \nmid k. \end{cases}$$

Proof. Indeed, if $p-1$ divides k, then $j^k \equiv 1 \pmod{p}$ for $j = 1, 2, \ldots , p-1$; so $S \equiv p-1 \equiv -1 \pmod{p}$. If $p-1$ does not divide k, let g be a primitive root modulo p. Then $g^k \not\equiv 1 \pmod{p}$. Since the sets of residue classes $\{1 \bmod p,\ 2 \bmod p, \ldots , (p-1) \bmod p\}$ and $\{g \bmod p,\ 2g \bmod p, \ldots , (p-1)g \bmod p\}$ are the same, then

$$g^k S \equiv \sum_{j=1}^{p-1}(gj)^k \equiv \sum_{j=1}^{p-1} j^k \equiv S \pmod{p}.$$

Hence $(g^k - 1)S \equiv 0 \pmod{p}$ and, since p does not divide $g^k - 1$, then $S \equiv 0 \pmod{p}$. □

The determination of a primitive root modulo p may be effected by a simple method indicated by Gauss in articles 73, 74 of *Disquisitiones Arithmeticae.*

Proceed as follows:

Step 1. Choose any integer a, $1 < a < p$, for example, $a = 2$, and write the residues modulo p of a, a^2, $a^3, \ldots$. Let t be the smallest exponent such that $a^t \equiv 1 \pmod{p}$. If $t = p-1$, then a is a primitive root modulo p. Otherwise, proceed to the next step.

Step 2. Choose any number b, $1 < b < p$, such that $b \not\equiv a^i \pmod{p}$ for $i = 1, \ldots , t$; let u be the smallest exponent such that $b^u \equiv 1 \pmod{p}$. It is simple to see that u cannot be a factor of t, otherwise $b^t \equiv 1 \pmod{p}$; but $1, a, a^2, \ldots , a^{t-1}$ are t pairwise incongruent solutions of the congruence $X^t \equiv 1 \pmod{p}$; so they are all the

possible solutions, and therefore $b \equiv a^m \pmod{p}$, for some m, $0 \le m \le t - 1$, which is contrary to the hypothesis. If $u = p - 1$, then b is a primitive root modulo p. If $u \ne p - 1$, let v be the least common multiple of t, u; so $v = mn$ with m dividing t, n dividing u, and $\gcd(m, n) = 1$. Let $a' \equiv a^{t/m} \pmod{p}$, $b' \equiv b^{u/n} \pmod{p}$ so $c = a'b'$ has order $mn = v$ modulo p. If $v = p - 1$, then c is a primitive root modulo p. Otherwise, proceed to the next step, which is similar to step 2.

Note that $v > t$, so in each step either one reaches a primitive root modulo p, or one constructs an integer with a bigger order modulo p. The process must stop; one eventually reaches an integer with order $p - 1$ modulo p, that is, a primitive root modulo p.

Gauss also illustrated the procedure with the example $p = 73$, and found that $g = 5$ is a primitive root modulo 73.

The above construction leads to a primitive root modulo p, but not necessarily to the smallest integer g_p, $1 < g_p < p$, which is a primitive root modulo p.

The determination of g_p is done by trying successively the various integers $a = 2, 3, \ldots$ and computing their orders modulo p. There is no uniform way of predicting, for all primes p, which is the smallest primitive root modulo p. However, several results were known about the size of g_p. In 1944, Pillai proved that there exist infinitely many primes p, such that $g_p > C \log \log p$ (where C is a positive constant). In particular, $\limsup_{p \to \infty} g_p = \infty$. A few years later, using a very deep theorem of Linnik (see Chapter 4) on primes in arithmetic progressions, Fridlender (1949), and independently Salié (1950), proved that $g_p > C \log p$, for some constant C and infinitely many primes p. On the other hand, g_p does not grow too fast, as proved by Burgess in 1962:

$$g_p \le C p^{1/4 + \varepsilon}$$

(for $\varepsilon > 0$, a constant $C > 0$, and p sufficiently large).

Grosswald made Burgess' result explicit in 1981: if $p > e^{e^{24}}$ then $g_p < p^{0.499}$.

The proof of the weaker result (with $1/2$ in place of $1/4$), attributed to Vinogradov, is in Landau's *Vorlesungen über Zahlentheorie*, Part VII, Chapter 14 (see General References).

The proof of the following result is elementary (problem proposed by Powell in 1983, solution by Kearnes in 1984):

For any positive integer M, there exist infinitely many primes p such that $M < g_p < p - M$.

As an illustration, the following table gives the smallest primitive root modulo p, for each prime $p < 1000$.

Table 1.   The smallest primitive root modulo p

p	g_p	p	g_p	p	g_p	p	g_p	p	g_p	p	g_p
2	1	127	3	283	3	467	2	661	2	877	2
3	2	131	2	293	2	479	13	673	5	881	3
5	2	137	3	307	5	487	3	677	2	883	2
7	3	139	2	311	17	491	2	683	5	887	5
11	2	149	2	313	10	499	7	691	3	907	2
13	2	151	6	317	2	503	5	701	2	911	17
17	3	157	5	331	3	509	2	709	2	919	7
19	2	163	2	337	10	521	3	719	11	929	3
23	5	167	5	347	2	523	2	727	5	937	5
29	2	173	2	349	2	541	2	733	6	941	2
31	3	179	2	353	3	547	2	739	3	947	2
37	2	181	2	359	7	557	2	743	5	953	3
41	6	191	19	367	6	563	2	751	3	967	5
43	3	193	5	373	2	569	3	757	2	971	6
47	5	197	2	379	2	571	3	761	6	977	3
53	2	199	3	383	5	577	5	769	11	983	5
59	2	211	2	389	2	587	2	773	2	991	6
61	2	223	3	397	5	593	3	787	2	997	7
67	2	227	2	401	3	599	7	797	2		
71	7	229	6	409	21	601	7	809	3		
73	5	233	3	419	2	607	3	811	3		
79	3	239	7	421	2	613	2	821	3		
83	2	241	7	431	7	617	3	823	3		
89	3	251	6	433	5	619	2	827	2		
97	5	257	3	439	15	631	3	829	2		
101	2	263	5	443	2	641	3	839	11		
103	5	269	2	449	3	643	11	853	2		
107	2	271	6	457	13	647	5	857	3		
109	6	277	5	461	2	653	2	859	2		
113	3	281	3	463	3	659	2	863	5		

A simple glance at the table suggests the following question: Is 2 a primitive root for infinitely many primes? More generally, if the integer $a \neq \pm 1$ is not a square, is it a primitive root modulo infinitely

many primes? This is a difficult problem and I shall return to it in Chapter 4.

B   THE THEOREM OF WILSON

Wilson's Theorem. *If p is a prime number, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. This is just a corollary of Fermat's little theorem. Indeed, $1, 2, \ldots, p-1$ are roots of the congruence $X^{p-1} - 1 \equiv 0 \pmod{p}$. But a congruence modulo p cannot have more roots than its degree. Hence,

$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod{p}.$$

Comparing the constant terms, $-1 \equiv (-1)^{p-1}(p-1)! = (p-1)!$ (mod p). (This is also true if $p = 2$.)   □

Wilson's theorem gives a characterization of prime numbers. Indeed, if $N > 1$ is a natural number that is not a prime, then $N = mn$, with $1 < m, n < N-1$, so m divides N and $(N-1)!$, and therefore $(N-1)! \not\equiv -1 \pmod{N}$.

However, Wilson's characterization of the prime numbers is not of practical value to test the primality of N, since there is no known algorithm to rapidly compute $N!$, say, in $\log N$ steps.

C   THE PROPERTIES OF GIUGA AND OF WOLSTENHOLME

Now, I shall consider other properties that are satisfied by prime numbers.

The property of Giuga

First, I note that if p is a prime, then by Fermat's little theorem (as already indicated)

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

In 1950, Giuga asked whether the converse is true: If $n > 1$ and n divides $1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} + 1$, then is n a prime number?

It is easy to show that n satisfies Giuga's condition if and only if, for every prime p dividing n, $p^2(p-1)$ divides $n-p$. Indeed, writing $n = pt$, Giuga's condition becomes

$$A = 1 + \sum_{j=1}^{pt-1} j^{pt-1} \equiv 0 \pmod{p},$$

while the condition that $p^2(p-1)$ divides $pt-p$ is equivalent to the conjunction of both conditions: $p \mid t-1$ and $p-1 \mid t-1$. But $pt-1 = (p-1)t + (t-1)$; hence, by Fermat's little theorem,

$$A \equiv 1 + \sum_{j=1}^{pt-1} j^{t-1} \equiv 1 + tS \pmod{p},$$

where $S = \sum_{j=1}^{p-1} j^{t-1}$. Hence,

$$A \equiv \begin{cases} 1 - t \pmod{p}, & \text{when} \quad p-1 \mid t-1 \\ 1 \pmod{p}, & \text{when} \quad p-1 \nmid t-1. \end{cases}$$

Thus, if $A \equiv 0 \pmod{p}$, then $p-1 \mid t-1$ and $p \mid t-1$. But, conversely, these latter conditions imply that $A \equiv 0 \pmod{p}$ and $p \nmid t$, so n is squarefree and therefore $A \equiv 0 \pmod{n}$.   □

It follows at once that $n \equiv p \equiv 1 \pmod{p-1}$; so, if $p \mid n$, then $p-1 \mid n-1$. A composite number n having this property is called a *Carmichael number*.

In Section IX, I shall indicate that this condition is severely restrictive. At any rate, it is now known that if there exists a composite integer n satisfying Giuga's condition, then n must have at least 12000 digits; see Bedocchi (1985) and Borwein, Borwein, Borwein & Girgensohn (1996).

The property of Wolstenholme

In 1862, Wolstenholme proved the following interesting result: If p is a prime, $p \geq 5$, then the numerator of

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p^2, and the numerator of

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}$$

is divisible by p.

For a proof, see Hardy & Wright (1938, p. 88, General References). Based on this property, it is not difficult to deduce that if $n \geq 5$ is a prime number, then

$$\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}.$$

Is the converse true? This question, still unanswered today, has been asked by J.P. Jones for many years. An affirmative reply would provide an interesting and formally simple characterization of prime numbers.

The problem leads naturally to the following concepts and questions. Let $n \geq 5$ be odd, and let

$$A(n) = \binom{2n-1}{n-1}.$$

For each $k \geq 1$ we may consider the set

$$W_k = \{n \text{ odd}, n \geq 5 \mid A(n) \equiv 1 \pmod{n^k}\}.$$

Thus $W_1 \supset W_2 \supset W_3 \supset W_4 \supset \ldots$. From Wolstenholme's theorem, every prime number greater than 3 belongs to W_3. Jones' question is whether W_3 is just the set of these prime numbers.

A prime number belonging to W_4 is called a *Wolstenholme prime*. Only two Wolstenholme primes are known today: 16843, indicated by Selfridge & Pollack in 1964, and 2124679, discovered by Crandall, Ernvall and Metsänkylä in 1993. In 1995, McIntosh determined by calculation that there is no other Wolstenholme prime $p < 5 \times 10^8$.

The set of composite integers in W_2 contains the squares of Wolstenholme's primes. McIntosh conjectured that these sets coincide and verified that this is true up to 10^9: the only composite $n \in W_2$, $n < 10^9$, is $n = 283686649 = 16843^2$.

It is believed, and was suggested by McIntosh, that there exist infinitely many Wolstenholme primes. The proof of this assertion would be very difficult.

D   THE POWER OF A PRIME DIVIDING A FACTORIAL

In 1808, Legendre determined the exact power p^m of the prime p that divides a factorial $a!$ (so p^{m+1} does not divide $a!$).

There is a very nice expression of m in terms of the p-adic development of a:

$$a = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p + a_0,$$

where $p^k \leq a < p^{k+1}$ and $0 \leq a_i \leq p-1$ (for $i = 0, 1, \ldots, k$). The integers $a_0, a_1, \ldots, a_k$ are the digits of a in base p.

For example, in base $5, 328 = 2 \times 5^3 + 3 \times 5^2 + 3$, so the digits of 328 in base 5 are 2, 3, 0, 3. Using the above notation:

Legendre's Theorem.

$$m = \sum_{i=1}^{\infty} \left[\frac{a}{p^i} \right] = \frac{a - (a_0 + a_1 + \cdots + a_k)}{p - 1}.$$

Proof. By definition $a! = p^m b$, where $p \nmid b$. Let $a = q_1 p + r_1$ with $0 \leq q_1$, $0 \leq r_1 < p$; so $q_1 = [a/p]$. The multiples of p, not bigger than a, are $p, 2p, \ldots, q_1 p \leq a$. So $p^{q_1}(q_1!) = p^m b'$, where $p \nmid b'$. Thus $q_1 + m_1 = m$, where p^{m_1} is the exact power of p which divides $q_1!$. Since $q_1 < a$, by induction,

$$m_1 = \left[\frac{q_1}{p} \right] + \left[\frac{q_1}{p^2} \right] + \left[\frac{q_1}{p^3} \right] + \cdots .$$

But

$$\left[\frac{q_1}{p^i} \right] = \left[\frac{[a/p]}{p^i} \right] = \left[\frac{a}{p^{i+1}} \right],$$

as may be easily verified. So

$$m = \left[\frac{a}{p} \right] + \left[\frac{a}{p^2} \right] + \left[\frac{a}{p^3} \right] + \cdots .$$

Now, I derive the second expression, involving the p-adic digits of $a = a_k p^k + \cdots + a_1 p + a_0$. Then

$$\left[\frac{a}{p}\right] = a_k p^{k-1} + \cdots + a_1,$$

$$\left[\frac{a}{p^2}\right] = a_k p^{k-2} + \cdots + a_2,$$

$$\vdots$$

$$\left[\frac{a}{p^k}\right] = a_k.$$

So

$$\sum_{i=0}^{\infty} \left[\frac{a}{p^i}\right] = a_1 + a_2(p+1) + a_3(p^2 + p + 1) + \cdots$$

$$+ a_k(p^{k-1} + p^{k-2} + \cdots + p + 1)$$

$$= \frac{1}{p-1}\left\{a_1(p-1) + a_2(p^2-1) + \cdots + a_k(p^k-1)\right\}$$

$$= \frac{1}{p-1}\left\{a - (a_0 + a_1 + \cdots + a_k)\right\}. \qquad \square$$

In 1852, Kummer used Legendre's result to determine the exact power p^m of p dividing a binomial coefficient

$$\binom{a+b}{a} = \frac{(a+b)!}{a!b!},$$

where $a \geq 1$, $b \geq 1$.

Let

$$a = a_0 + a_1 p + \cdots + a_t p^t,$$
$$b = b_0 + b_1 p + \cdots + b_t p^t,$$

where $0 \leq a_i \leq p-1$, $0 \leq b_i \leq p-1$, and either $a_t \neq 0$ or $b_t \neq 0$. Let $S_a = \sum_{i=0}^{t} a_i$, $S_b = \sum_{i=0}^{t} b_i$ be the sums of p-adic digits of a, b. Let c_i, $0 \leq c_i \leq p-1$, and $\varepsilon_i = 0$ or 1, be defined successively as follows:

$$a_0 + b_0 = \varepsilon_0 p + c_0,$$
$$\varepsilon_0 + a_1 + b_1 = \varepsilon_1 p + c_1,$$
$$\vdots$$
$$\varepsilon_{t-1} + a_t + b_t = \varepsilon_t p + c_t.$$

Multiplying these equations successively by 1, p, $p^2, \ldots$ and adding them:

$$a + b + \varepsilon_0 p + \varepsilon_1 p^2 + \cdots + \varepsilon_{t-1} p^t$$
$$= \varepsilon_0 p + \varepsilon_1 p^2 + \cdots + \varepsilon_{t-1} p^t + \varepsilon_t p^{t+1} + c_0 + c_1 p + \cdots + c_t p^t.$$

So, $a + b = c_0 + c_1 p + \cdots + c_t p^t + \varepsilon_t p^{t+1}$, and this is the expression of $a + b$ in the base p. Similarly, by adding those equations:

$$S_a + S_b + (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_{t-1}) = (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_t)p + S_{a+b} - \varepsilon_t.$$

By Legendre's result

$$(p-1)m = (a+b) - S_{a+b} - a + S_a - b + S_b$$
$$= (p-1)(\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_t).$$

Hence the following result:

Kummer's Theorem. *The exponent of the exact power of p dividing $\binom{a+b}{a}$ is equal to $\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_t$, which is the number of "carry-overs" when performing the addition of a, b, written in the base p.*

This theorem of Kummer was rediscovered by Lucas in 1878. In 1991, Frasnay extended the result replacing integers by p-adic integers.

The results of Legendre and Kummer have found many applications, in p-adic analysis, and also, for example, in Chapter 3, Section III.

E   THE CHINESE REMAINDER THEOREM

Even though my paramount interest is in prime numbers, there is no way to escape dealing with arbitrary integers also—which essentially amounts, in many questions, to the simultaneous consideration of several primes, because of the decomposition, in a unique way, of integers into the product of prime powers.

One of the keys connecting results for integers n, and for their prime power factors, is very old; indeed, it was known to the ancient Chinese, and it is therefore called the Chinese remainder theorem.

However, according to A. Zachariou (private communication) it was known even before them by the Greeks, but since the Greeks

discovered so many theorems, I will keep the traditional name for this one. I am sure that every one of my readers knows it already:

If $n_1, n_2, \ldots, n_k$ are pairwise relatively prime integers, greater than 1, and if $a_1, a_2, \ldots, a_k$ are any integers, then there exists an integer a such that

$$\begin{cases} a \equiv a_1 \pmod{n_1} \\ a \equiv a_2 \pmod{n_2} \\ \quad\vdots \\ a \equiv a_k \pmod{n_k}. \end{cases}$$

Another integer a' also satisfies the same congruences as a if and only if $a \equiv a' \pmod{n_1 n_2 \cdots n_k}$. So, there exists a unique integer a, as above, with $0 \le a < n_1 n_2 \cdots n_k$.

The proof is indeed very simple; it is in many books and also in a short note by Mozzochi (1967).

The Chinese remainder theorem has numerous applications. It is conceivable that one of these might have been the way the Chinese generals counted their troops:

Line up 7 by 7!   (Not factorial of 7, but a SCREAMED military command.)

Line up 11 by 11!

Line up 13 by 13!

Line up 17 by 17!

Counting only the remainders in the incomplete rows, the intelligent generals could know the exact number of their soldiers.[1]

Here is another application of the Chinese remainder theorem. If $n = p_1 p_2 \cdots p_k$ is a product of distinct primes, if g_i is a primitive root modulo p_i (for each i), if g is such that $1 \le g \le n - 1$ and $g \equiv g_i \pmod{p_i}$ for every $i = 1, 2, \ldots, k$, then the order of g modulo p_i is $p_i - 1$ for each $i = 1, 2, \ldots, k$ and the order of g modulo n is $\prod_{i=1}^{k}(p_i - 1)$.

---

[1] In between us, this may never have been practiced. The existence of intelligent generals remains a wide open question.

F EULER'S FUNCTION

Euler generalized Fermat's little theorem by introducing the *totient* or *Euler's function*.

For every $n \geq 1$, let $\varphi(n)$ denote the number of integers a, $1 \leq a < n$, such that $\gcd(a, n) = 1$. Thus, if $n = p$ is a prime, then $\varphi(p) = p - 1$; also

$$\varphi(p^k) = p^{k-1}(p-1) = p^k \left(1 - \frac{1}{p}\right).$$

Moreover, if $m, n \geq 1$ and $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$, that is, φ is a multiplicative function. Hence, for any integer $n = \prod_p p^k$ (product for all primes p dividing n, and $k \geq 1$), then

$$\varphi(n) = \prod_p p^{k-1}(p-1) = n \prod_p \left(1 - \frac{1}{p}\right).$$

Another simple property is: $n = \sum_{d|n} \varphi(d)$.
Euler proved the following:

Euler's Theorem. *If* $\gcd(a, n) = 1$, *then* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof. Let $r = \varphi(n)$ and let $b_1, \ldots, b_r$ be integers, pairwise incongruent modulo n, such that $\gcd(b_i, n) = 1$ for $i = 1, \ldots, r$.

Then $ab_1, \ldots, ab_r$ are again pairwise incongruent modulo n and $\gcd(ab_i, n) = 1$ for $i = 1, \ldots, r$. Therefore, the sets $\{b_1 \bmod n, \ldots, b_r \bmod n\}$ and $\{ab_1 \bmod n, \ldots, ab_r \bmod n\}$ are equal. Now,

$$a^r \prod_{i=1}^{r} b_i \equiv \prod_{i=1}^{r} ab_i \equiv \prod_{i=1}^{r} b_i \pmod{n}.$$

Hence,

$$(a^r - 1) \prod_{i=1}^{r} b_i \equiv 0 \pmod{n} \quad \text{and so} \quad a^r \equiv 1 \pmod{n}. \qquad \square$$

Just like for Fermat's little theorem, it follows also from Euler's theorem that there exists the smallest positive exponent e such that $a^e \equiv 1 \pmod{n}$. It is called the *order of a modulo n*. If n is a prime number, this definition coincides with the previous one. Note also

that $a^m \equiv 1 \pmod{n}$ if and only if m is a multiple of the order e of a mod n; thus, in particular, e divides $\varphi(n)$.

Once again, it is natural to ask: Given $n > 2$ does there always exist an integer a, relatively prime to n, such that the order of a mod n is equal to $\varphi(n)$? Recall that when $n = p$ is a prime, such numbers exist, namely, the primitive roots modulo p. If $n = p^e$, a power of an odd prime, it is also true. More precisely, the following assertions are equivalent:

(i) g is a primitive root modulo p and $g^{p-1} \not\equiv 1 \pmod{p^2}$;

(ii) g is a primitive root modulo p^2;

(iii) for every $e \geq 2$, g is a primitive root modulo p^e.

Note that 10 is a primitive root modulo 487, but $10^{486} \equiv 1 \pmod{487^2}$, so 10 is not a primitive root modulo 487^2. This is the smallest example illustrating this possibility, when the base is 10. Another example is 14 modulo 29.

However, if n is divisible by $4p$, or pq, where p, q are distinct odd primes, then there is no number a, relatively prime to n, with order equal to $\varphi(n)$. Indeed, it is easy to see that the order of a mod n is at most equal to $\lambda(n)$, where $\lambda(n)$ is the following function, defined by Carmichael in 1912:

$$\lambda(1) = 1,\ \lambda(2) = 1,\ \lambda(4) = 2,$$

$$\lambda(2^r) = 2^{r-2} \quad \text{(for } r \geq 3\text{)},$$

$$\lambda(p^r) = p^{r-1}(p-1) = \varphi(p^r) \quad \begin{array}{l} \text{for any odd prime } p \\ \text{and } r \geq 1, \end{array}$$

$$\lambda\big(2^r p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}\big) = \operatorname{lcm}\big\{\lambda(2^r), \lambda(p_1^{r_1}), \ldots, \lambda(p_s^{r_s})\big\}$$

(lcm denotes the least common multiple).

Note that $\lambda(n)$ divides $\varphi(n)$, but may be smaller, and that there is an integer a, relatively prime to n, with order of a mod n equal to $\lambda(n)$.

I shall use this opportunity to study Euler's function in more detail. First I shall consider Lehmer's problem, and thereafter the values of φ, the valence, the values avoided, the average of the function, etc.

Lehmer's problem

Recall that if p is a prime, then $\varphi(p) = p - 1$. In 1932, Lehmer asked whether there exists any composite integer n such that $\varphi(n)$ divides $n - 1$. This question remains open and its solution seems as remote today as it was when Lehmer raised it seven decades ago. If the answer is negative, it will provide a characterization of prime numbers.

What can one say, anyway, when it is not possible to solve the problem? Only that the existence of composite integers n, for which $\varphi(n)$ divides $n - 1$, is unlikely, for various reasons:

(a) any such number must be very large (if it exists at all);

(b) any such number must have many prime factors (if it exists at all);

(c) the number of such composite numbers, smaller than any given real number x, is bounded by a very small function of x.

Thus, Lehmer showed in 1932 that if n is composite and $\varphi(n)$ divides $n - 1$, then n is odd and square-free, and the number of its distinct prime factors is $\omega(n) \geq 7$. Subsequent work by Schuh (1944) gave $\omega(n) \geq 11$. In 1970, Lieuwens showed that if $3 \mid n$, then $\omega(n) \geq 213$ and $n > 5.5 \times 10^{570}$; if $30 \nmid n$, then $\omega(n) \geq 13$.

RECORD

In 1980, Cohen and Hagis showed that if n is composite and $\varphi(n)$ divides $n - 1$, then $n > 10^{20}$ and $\omega(n) \geq 14$. Wall (1980) showed that if $\gcd(30, n) = 1$, then $\omega(n) \geq 26$, while if $3 \mid n$, the best result is still Lieuwens'.

In 1977, Pomerance showed that for every sufficiently large positive real number x, the number $L(x)$ of composite n such that $\varphi(n)$ divides $n - 1$ and $n \leq x$, satisfies

$$L(x) \leq x^{1/2}(\log x)^{3/4}.$$

Moreover, if $\omega(n) = k$, then $n < k^{2^k}$.

Values of Euler's function

Not every even integer $m > 1$ is a value of Euler's function—a fact which is not difficult to establish. For example, Schinzel showed in 1956 that, for every $k \geq 1$, 2×7^k is not a value of Euler's function.

In 1976, Mendelsohn showed that there exist infinitely many primes p such that, for every $k \geq 1$, $2^k p$ is not a value of the function φ. Concerning interesting values assumed by Euler's function, Erdös in 1946 proposed as a problem to show that for every $k \geq 1$ there exists n such that $\varphi(n) = k!$. A solution by Lambek was proposed in 1948; the same result was given later by Gupta (1950).

The next results tell how erratic is the behaviour of Euler's function. Thus, in 1950, Somayajulu showed that

$$\limsup_{n \to \infty} \frac{\varphi(n+1)}{\varphi(n)} = \infty \quad \text{and} \quad \liminf_{n \to \infty} \frac{\varphi(n+1)}{\varphi(n)} = 0.$$

This result was improved by Schinzel and Sierpiński, see Schinzel (1954): the set of all numbers $\varphi(n+1)/\varphi(n)$ is dense in the set of all real positive numbers.

Schinzel & Sierpiński (1954) and Schinzel (1954) also proved the following:

For every m, $k \geq 1$, there exist n, $h \geq 1$ such that

$$\frac{\varphi(n+i)}{\varphi(n+i-1)} > m \quad \text{and} \quad \frac{\varphi(h+i-1)}{\varphi(h+i)} > m$$

for $i = 1, 2, \dots, k$. It is also true that the set of all numbers $\varphi(n)/n$ is dense in the interval $(0, 1)$.

The valence of Euler's function

Now I shall examine the "valence" of Euler's function; in other words, how often a value $\varphi(n)$ is assumed. In order to explain the results in a systematic way, it is better to introduce some notation. If $m \geq 1$, let

$$V_\varphi(m) = \#\{n \geq 1 \mid \varphi(n) = m\}.$$

What are the possible values of $V_\varphi(m)$? I have already said that there are infinitely many even integers m for which $V_\varphi(m) = 0$. It is also true that if $m = 2 \times 3^{6k+1}$ ($k \geq 1$), then $\varphi(n) = m$ exactly when $n = 3^{6k+2}$ or $n = 2 \times 3^{6k+2}$. Hence, there are infinitely many integers m such that $V_\varphi(m) = 2$.

It is not difficult to show that $V_\varphi(m) \neq \infty$ for every $m \geq 1$.

Schinzel gave a simpler proof (in 1956) of the following result of Pillai (1929):

$$\sup\{V_\varphi(m)\} = \infty.$$

In other words, for every $k \geq 1$ there exists an integer m_k such that there exist at least k integers n with $\varphi(n) = m_k$.

The above result is weaker than the long-standing conjecture of Sierpiński: For every integer $k \geq 2$ there exists $m > 1$ such that $k = V_\varphi(m)$. With very sophisticated methods, this conjecture has now been proved by Ford (1999).

Carmichael's conjecture

The conjecture that dominates the study of the valence of φ was proposed by Carmichael in 1922: V_φ does not assume the value 1. In other words, given $n \geq 1$, there exists $n' \geq 1$, $n' \neq n$, such that $\varphi(n') = \varphi(n)$.

This conjecture was studied by Klee, who showed in 1947 that it holds for every integer n such that $\varphi(n) < 10^{400}$. Masai & Valette (1982), using Klee's method, showed that $\varphi(n) < 10^{10000}$. In 1994, still basically using Klee's method, but with extensive calculations, Schlafly & Wagon have brilliantly increased the lower bound for a counterexample to Carmichael's conjecture: if $V_\varphi(n) = 1$, so $n > 10^{10^7}$. With much more powerful methods, Ford (1998) further improved the lower bound to reach $n > 10^{10^{10}}$.

An article about Carmichael's conjecture, also written by Wagon, had appeared earlier in *The Mathematical Intelligencer* (1986). Numerical evidence points to the truth of Carmichael's conjecture. However, Pomerance (1974) has shown the following: Suppose that m is a natural number such that if p is any prime and $p-1$ divides $\varphi(m)$, then p^2 divides m. Then $V_\varphi(\varphi(m)) = 1$.

Of course, if there exists a number m satisfying the above condition, then Carmichael's conjecture would be false. However, the existence of such a number m is far from established, and perhaps unlikely.

The most important recent work on Carmichael's conjecture is due to K. Ford (1998). For every $x > 0$ let $E(x) = \#\{n \mid 1 \leq n < x$ such that there exists $k > 1$ with $\varphi(k) = n\}$ and $E_1(x) = \#\{n \mid 1 \leq n < x$ such that there exists a unique k with $\varphi(k) = n\}$. Carmichael's conjecture says that $E_1(x) = 0$ for every $x > 0$. Ford showed that if

Carmichael's conjecture is false, then there exists $C > 0$ such that for every sufficiently large x we have $E(x) \leq C\, E_1(x)$. It follows that Carmichael's conjecture is equivalent to the statement

$$\liminf_{x \to \infty} \frac{E_1(x)}{E(x)} = 0.$$

Ford also showed that $E_1(10^{10^{10}}) = 0$.

Finally, in variance with Carmichael's conjecture, it is reasonable to expect that every $s > 1$ is a value of V_φ; this was conjectured by Sierpiński. As a matter of fact, I shall indicate in Chapter 6, Section II, that this statement follows from an unproved and very interesting hypothesis.

And how about the valence of the valence function V_φ? I have already said that there exist infinitely many m that are not values of φ, for which $V_\varphi(m) = 0$. So V_φ assumes the value 0 infinitely often.

This was generalized by Erdös in 1958: If $s \geq 1$ is a value of V_φ, then it is assumed infinitely often. (Try to phrase this statement directly using Euler's function, to see whether you understand my notation.)

The growth of Euler's function

I have not yet considered the growth of the function φ. Since $\varphi(p) = p - 1$ for every prime p, then $\limsup \varphi(n) = \infty$. Similarly, from $\varphi(p) = p - 1$, $\limsup \varphi(n)/n = 1$.

I shall postpone the indication of other results about the growth of φ until Chapter 4: they depend on methods that will be discussed in that chapter.

G   Sequences of Binomials

The preceding considerations referred to congruences modulo a given integer $n > 1$, and a was any positive integer relatively prime to n.

Another point of view is very illuminating. This time, let $a > 1$ be given, and consider the sequence of integers $a^n - 1$ (for $n \geq 1$), as well as the companion sequence of integers $a^n + 1$ (for $n \geq 1$). More generally, if $a > b \geq 1$ with $\gcd(a, b) = 1$, one may consider the sequences $a^n - b^n$ $(n \geq 1)$ and $a^n + b^n$ $(n \geq 1)$.

A first natural question, with an immediate answer, is the following: to determine all primes p, such that there exists $n \geq 1$ for which

p divides $a^n - b^n$. These are primes p not dividing ab because a, b are relatively prime. Conversely, if $p \nmid ab$, if $bb' \equiv 1 \pmod{p}$ and n is the order of $ab' \bmod p$, then p divides $a^n - b^n$.

It is more complicated for the binomials $a^n + b^n$. If $p \neq 2$ and there exists $n \geq 1$ such that p divides $a^n + b^n$, then $p \nmid ab(a - b)$. The converse is false; for example, 7 does not divide $2^n + 1$ for every $n \geq 1$.

Primitive prime factors

If $n \geq 1$ is the smallest integer such that p divides $a^n - b^n$ (resp. $a^n + b^n$), then p is called a *primitive prime factor* of the sequence of binomials in question. In this case, by Fermat's little theorem, n divides $p - 1$; this was explicitly observed by Legendre.

So, every prime $p \nmid ab$ appears as a primitive factor of some binomial $a^n - b^n$. Does, conversely, every binomial have a primitive factor?

In 1892, Zsigmondy proved the following theorem, which is very interesting and has many applications:

If $a > b \geq 1$ and $\gcd(a, b) = 1$, then every number $a^n - b^n$ has a primitive prime factor—the only exceptions being $a - b = 1$, $n = 1$; $2^6 - 1 = 63$; and $a^2 - b^2$, where a, b are odd and $a + b$ is a power of 2.

Equally, if $a > b \geq 1$, then every number $a^n + b^n$ has a primitive prime factor—with the exception of $2^3 + 1 = 9$.

The special case, where $b = 1$, had been proved by Bang in 1886. Later, this theorem, or Bang's special case, was proved again, sometimes unknowingly, by a long list of mathematicians: Birkhoff & Vandiver (1904), Carmichael (1913), Kanold (1950), Artin (1955), Lüneburg (1981), and probably others.

The proof is definitely not so obvious; however, it is very easy to write up such sequences and watch the successive appearance of new primitive prime factors.

It is interesting to consider the primitive part t_n^* of $a^n - b^n$; namely, write $a^n - b^n = t_n^* t_n'$ with $\gcd(t_n^*, t_n') = 1$ and a prime p divides t_n^* if and only if p is a primitive factor of $a^n - b^n$.

By experimenting numerically with sequences $a^n - b^n$, it is observed that, apart from a few initial terms, t_n^* is composite. In fact, Schinzel indicated the following theorem in 1962.

Let $k(m)$ denote the square-free kernel of m, that is, m divided by its largest square factor. Let

$$
e = \begin{cases} 1, & \text{if } k(ab) \equiv 1 \pmod 4, \\ 2, & \text{if } k(ab) \equiv 2 \text{ or } 3 \pmod 4. \end{cases}
$$

If $n/ek(ab)$ is integral and odd, and if $n > 1$, then $a^n - b^n$ has at least two distinct primitive prime factors, with only a few exceptions (of which the largest possible is $n = 20$). When $n > 1$ and $b = 1$, the exceptions are:

$$
\begin{aligned}
\text{if } a = 2: & \quad n = 4, 12, 20; \\
\text{if } a = 3: & \quad n = 6; \\
\text{if } a = 4: & \quad n = 3.
\end{aligned}
$$

Therefore, there are infinitely many n such that the primitive part of $a^n - b^n$ is composite.

Schinzel also proved that if $ab = c^h$ with $h \geq 3$, or $h = 2$ and $k(c)$ odd, then there are infinitely many n such that the primitive part of $a^n - b^n$ has at least three prime factors.

For the sequence of binomials $a^n + b^n$, it follows at once that if $n/ek(ab)$ is odd, and $n > 10$, then the primitive part of $a^n + b^n$ is composite. Just note that each primitive prime factor of $a^{2n} - b^{2n}$ is also a primitive prime factor of $a^n + b^n$.

Here are some questions that are very difficult to answer:

Are there infinitely many n such that the primitive part of $a^n - b^n$ is prime?

Are there infinitely many n such that the primitive part $a^n - b^n$ is square-free?

And how about the seemingly easier questions:

Are there infinitely many n such that the primitive part t_n^* of $a^n - b^n$ has a prime factor p such that p^2 does not divide $a^n - b^n$?

Are there infinitely many n such that t_n^* has a square-free kernel $k(t_n^*) \neq 1$?

These questions, for the special case when $b = 1$, are ultimately related, in a very surprising way, to Fermat's last theorem!

The largest prime factor

It is also an interesting problem to estimate the size of the largest prime factor of $a^n - b^n$, where $a > b \geq 1$ and $\gcd(a, b) = 1$. The following notation will be used: $P[m]$ designates the largest prime factor of $m \geq 1$.

It is not difficult to show, using Zsigmondy's theorem, that $P[a^n - b^n] \geq n + 1$ when $n > 2$.

In 1962, Schinzel showed that $P[a^n - b^n] \geq 2n + 1$ in the following cases, with $n > 2$: $4 \nmid n$, with exclusion $a = 2$, $b = 1$, $n = 6$; $k(ab) \mid n$ or $k(ab) = 2$, with exclusions $a = 2$, $b = 1$, $n = 4, 6$, or 12.

Erdös conjectured in 1965 that $\lim_{n\to\infty} P[2^n - 1]/n = \infty$. Despite very interesting work, this conjecture has not yet been settled completely; but there are very good partial results, which I report now.

In 1975, using Baker's inequalities for linear forms of logarithms, Stewart showed the following. Let $0 < r < 1/\log 2$, and let S_r be the set of integers n having at most $r \log \log n$ distinct prime factors (the set S_r has density 1); then

$$\lim_{\substack{n\to\infty \\ n\in S_r}} \frac{P[a^n - b^n]}{n} = \infty.$$

How fast does the expression increase? This was answered by Stewart in 1977, with sharper inequalities of Baker's type:

$$\frac{P[a^n - b^n]}{n} > C \frac{(\log n)^\lambda}{\log \log \log n},$$

where $\lambda = 1 - r \log 2$, $C > 0$ is a convenient constant, and $n \in S_r$.

Stewart also showed that, for every sufficiently large prime p, $P[a^p - b^p]/p > C \log p$ ($C > 0$). The special case of Mersenne numbers $2^p - 1$ had been established in 1976 by Erdös and Shorey.

There is also a close connection between the numbers $a^n - 1$, the values of the cyclotomic polynomials, and primes in certain arithmetic progressions, but I cannot explain everything at the same time—so be patient and wait until I consider this matter again in Chapter 4, Section IV.

H   QUADRATIC RESIDUES

In the study of quadratic diophantine equations, developed by Fermat, Euler, Legendre, and Gauss, it was very important to determine when an integer a is a square modulo a prime $p > 2$.

If $p > 2$ does not divide a, and if there exists an integer b such that $a \equiv b^2 \pmod{p}$, then a is called a *quadratic residue modulo p*; otherwise, it is a *nonquadratic residue modulo p*.

Legendre introduced the following practical notation:

$$\left(\frac{a}{p}\right) = (a \mid p) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

It is also convenient to define $(a \mid p) = 0$ when p divides a.

I shall now indicate the most important properties of the Legendre symbol. References are plentiful—practically every book in elementary number theory.

If $a \equiv a' \pmod{p}$, then

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right).$$

For any integers a, a':

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right).$$

So, for the computation of the Legendre symbol, it suffices to calculate $(q \mid p)$, where $q = -1$, 2, or any odd prime different from p.

Euler proved the following congruence:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

In particular,

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{when } p \equiv 1 \pmod{4}, \\ -1 & \text{when } p \equiv -1 \pmod{4}, \end{cases}$$

and

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{when } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{when } p \equiv \pm 3 \pmod{8}. \end{cases}$$

The computation of the Legendre symbol $(q \mid p)$, for any odd prime $q \neq p$, can be performed with an easy, explicit, and fast algorithm (needing only Euclidean division), by using Gauss' *reciprocity law*:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}.$$

The importance of Legendre's symbol was such that it prompted Jacobi to consider the following generalization, now called the Jacobi symbol. Again, references are abundant, for example, Grosswald's book (1966, 2nd edition 1984), or (why not?) my own book (1972, enlarged edition 2001).

Let a be a nonzero integer, and let b be an odd integer, such that $\gcd(a, b) = 1$. The Jacobi symbol $(a \mid b)$ is defined as an extension of Legendre's symbol, in the following manner. Let $b = \prod_{p \mid b} p^{e_p} > 0$ (with $e_p \geq 1$). Then

$$\left(\frac{a}{b}\right) = \prod_{p \mid b} \left(\frac{a}{p}\right)^{e_p},$$

$$\left(\frac{a}{-b}\right) = \begin{cases} \left(\dfrac{a}{b}\right), & \text{if } a > 0, \\ -\left(\dfrac{a}{b}\right), & \text{if } a < 0. \end{cases}$$

Therefore, $(a \mid b)$ is equal to $+1$ or -1. Note that

$$\left(\frac{a}{1}\right) = \left(\frac{a}{-1}\right) = +1 \quad \text{when } a > 0.$$

Here are some of the properties of the Jacobi symbol (under the assumptions of its definition):

$$\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right),$$

$$\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$$

$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2} = \begin{cases} +1 & \text{if } b \equiv 1 \pmod{4}, \\ -1 & \text{if } b \equiv -1 \pmod{4}, \end{cases}$$

$$\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8} = \begin{cases} +1 & \text{if } b \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } b \equiv \pm 3 \pmod{8}. \end{cases}$$

For the calculation of the Jacobi symbol, the key result is the reciprocity law, which follows easily from Gauss' reciprocity law for the Legendre symbol:

If a, b are relatively prime odd integers, then

$$\left(\frac{a}{b}\right) = \varepsilon \left(\frac{b}{a}\right) (-1)^{\frac{a-1}{2} \times \frac{b-1}{2}},$$

where

$$\varepsilon = \begin{cases} +1 & \text{if } a > 0 \text{ or } b > 0 \\ -1 & \text{if } a < 0 \text{ and } b < 0. \end{cases}$$

Finally, if $b \geq 3$, and if a is a square modulo b, then $(a \mid b) = +1$.

III   Classical Primality Tests Based on Congruences

After the discussion of the theorems of Fermat, Wilson, and Euler, I am ready. For me, the classical primality tests based on congruences are those indicated by Lehmer, extending or using previous tests by Lucas, Pocklington, and Proth. I reserve another section for classical tests based on recurring sequences.

Wilson's theorem, which characterizes prime numbers, might seem very promising, but it has to be discarded as a practical test, since the computation of factorials is very time consuming.

Fermat's little theorem says that if p is a prime and a is any natural number not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$. However, I note right away that a crude converse of this theorem is not true—because there exist composite integers N, and $a \geq 2$, such that $a^{N-1} \equiv 1 \pmod{N}$. I shall devote Section VIII to the study of these numbers, which are very important in primality questions.

Nevertheless, a true converse of Fermat's little theorem was discovered by Lucas in 1876. It says:

Test 1. Let $N > 1$. Assume that there exists an integer $a > 1$ such that:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^m \not\equiv 1 \pmod{N}$ for $m = 1, 2, \ldots, N - 2$.

Then N is a prime.

Defect of this test: it might seem perfect, but it requires $N-2$ successive multiplications by a, and finding residues modulo N—too many operations.

Proof. It suffices to show that every integer m, $1 \leq m < N$, is prime to N, that is, $\varphi(N) = N - 1$. For this purpose, it suffices to show that there exists a, $1 \leq a < N$, $\gcd(a, N) = 1$, such that the order of $a \bmod N$ is $N - 1$. This is exactly spelled out in the hypothesis. $\square$

In 1891, Lucas gave the following test:

Test 2. Let $N > 1$. Assume that there exists an integer $a > 1$ such that:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^m \not\equiv 1 \pmod{N}$ for every $m < N$, such that m divides $N-1$.

Then N is a prime.

Defect of this test: it requires the knowledge of all factors of $N-1$, thus it is only easily applicable when $N - 1$ can be factored, like $N = 2^n + 1$, or $N = 3 \times 2^n + 1$.

The proof of Test 2 is, of course, the same as that of Test 1.

In 1967, Brillhart & Selfridge made Lucas' test more flexible; see also the paper by Brillhart, Lehmer & Selfridge in 1975:

Test 3. Let $N > 1$. Assume that for every prime factor q of $N - 1$ there exists an integer $a = a(q) > 1$ such that

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $a^{(N-1)/q} \not\equiv 1 \pmod{N}$.

Then N is a prime.

Defect of this test: once again, it is necessary to know the prime factors of $N - 1$, but fewer congruences have to be satisfied.

An observant reader should note that, after all, to verify that $a^{N-1} \equiv 1 \pmod{N}$ it is necessary in particular to calculate, as one goes, the residue of a^n modulo N (for every $n \leq N - 1$), and so the first Lucas test could have been used. The point is that there is

a fast algorithm to find the power a^n, hence also $a^n \bmod N$, without computing all the preceding powers. It runs as follows.

Write the exponent n in base 2:

$$n = n_0 2^k + n_1 2^{k-1} + \cdots + n_{k-1} 2 + n_k,$$

where each n_i is equal to 0 or 1, and $n_0 = 1$.

Define the integers $r_0, r_1, r_2, \ldots$ successively, putting $r_0 = a$ and, for $j \geq 0$:

$$r_{j+1} = \begin{cases} r_j^2 & \text{if} \quad n_{j+1} = 0, \\ a r_j^2 & \text{if} \quad n_{j+1} = 1. \end{cases}$$

Then $a^n = r_k$.

So, it is only necessary to perform at most $2k$ operations, which are either a squaring or a multiplication by a. If the computation is of $a^n \bmod N$, then it is even easier; at each stage r_j is to be replaced by its residue modulo N. Now, k is equal to

$$\left[\frac{\log n}{\log 2} \right].$$

Therefore, if $n = N - 1$, then only about

$$2 \left[\frac{\log N}{\log 2} \right]$$

operations are needed to find $a^{N-1} \bmod N$, and there is no requirement of computing all powers $a^n \bmod N$.

Why don't you try calculating $2^{1092} \bmod 1093^2$ in this way? You should find $2^{1092} \equiv 1 \pmod{1093^2}$—if you really succeed! This has nothing to do directly with primality—but it will appear much later, in Chapter 5.

I return to Brillhart and Selfridge's Test 3 and give its proof.

Proof of Test 3. It is enough to show that $\varphi(N) = N - 1$, and since $\varphi(N) \leq N - 1$, it suffices to show that $N - 1$ divides $\varphi(N)$. If this is false, there exists a prime q and $r \geq 1$ such that q^r divides $N - 1$, but q^r does not divide $\varphi(N)$. Let $a = a(q)$ and let e be the order of $a \bmod N$. Thus e divides $N - 1$ and e does not divide $(N - 1)/q$, so q^r divides e. Since $a^{\varphi(N)} \equiv 1 \pmod{N}$, then e divides $\varphi(N)$, so $q^r \mid \varphi(N)$, which is a contradiction, and concludes the proof.   □

In the section on Fermat numbers, I will derive Pepin's primality test for Fermat numbers, as a consequence of Test 3.

To make the primality tests more efficient, it is desirable to avoid the need to find all prime factors of $N - 1$. So there are tests that only require a partial factorization of $N - 1$. The basic result was proved by Pocklington in 1914, and it is indeed very simple:

Let $N - 1 = q^n R$, where q is a prime, $n \geq 1$, and q does not divide R. Assume that there exists an integer $a > 1$ such that:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $\gcd(a^{(N-1)/q} - 1, N) = 1$.

Then each prime factor of N is of the form $mq^n + 1$, with $m \geq 1$.

Proof. Let p be a prime factor of N, and let e be the order of a mod p, so e divides $p - 1$; by condition (ii), e cannot divide $(N-1)/q$, because p divides N; hence, q does not divide $(N-1)/e$; so q^n divides e, and a fortiori, q^n divides $p - 1$. □

The above statement looks more like a result on factors than a primality test. However, if it may be verified that each prime factor $p = mq^n + 1$ is greater than $\sqrt{N}$, then N is a prime. When q^n is fairly large, this verification is not too time consuming.

Pocklington gave also the following refinement of his result above:

Let $N - 1 = FR$, where $\gcd(F, R) = 1$ and the factorization of F is known. Assume that for every prime q dividing F there exists an integer $a = a(q) > 1$ such that:

(i) $a^{N-1} \equiv 1 \pmod{N}$,

(ii) $\gcd(a^{(N-1)/q} - 1, N) = 1$.

Then each prime factor of N is of the form $mF + 1$, with $m \geq 1$.

The same comments apply here. So, if $F > \sqrt{N}$, then N is a prime.

This result is very useful to prove the primality of numbers of certain special form. The old criterion of Proth (1878) is easily deduced:

Test 4. Let $N = 2^n h + 1$ with h odd and $2^n > h$. Assume that there exists an integer $a > 1$ such that $a^{(N-1)/2} \equiv -1 \pmod{N}$. Then N is prime.

Proof. $N - 1 = 2^n h$, with h odd and $a^{N-1} \equiv 1 \pmod{N}$. Since N is odd, then $\gcd(a^{(N-1)/2} - 1, N) = 1$. By the above result, each prime factor p of N is of the form $p = 2^n m + 1 > 2^n$. But $N = 2^n h + 1 < 2^{2n}$, hence $\sqrt{N} < 2^n < p$ and so N is prime. □

In the following test (using the same notation) it is required to know that R (the nonfactored part of $N - 1$) has no prime factor less than a given bound B. Precisely:

Test 5. Let $N - 1 = FR$, where $\gcd(F, R) = 1$, the factorization of F is known, B is such that $FB > \sqrt{N}$, and R has no prime factors less than B. Assume:

(i) For each prime q dividing F there exists an integer $a = a(q) > 1$ such that $a^{N-1} \equiv 1 \pmod{N}$ and $\gcd(a^{(N-1)/q} - 1, N) = 1$.

(ii) There exists an integer $b > 1$ such that $b^{N-1} \equiv 1 \pmod{N}$ and $\gcd(b^F - 1, N) = 1$.

Then N is a prime.

Proof. Let p be any prime factor of N, let e be the order of b modulo N, so e divides $p - 1$ and also e divides $N - 1 = FR$. Since e does not divide F, then $\gcd(e, R) \neq 1$, so there exists a prime q such that $q \mid e$ and $q \mid R$; hence, $q \mid p - 1$. However, by the previous result of Pocklington, F divides $p - 1$; since $\gcd(F, R) = 1$, then qF divides $p - 1$. So $p - 1 \geq qF \geq BF > \sqrt{N}$. This implies that $p = N$, so N is a prime. □

The paper of Brillhart, Lehmer & Selfridge (1975) contains other variants of these tests, which have been put to good use to determine the primality of numbers of the form $2^r + 1$, $2^{2r} \pm 2^r + 1$, $2^{2r-1} \pm 2^r + 1$.

I have already said enough and will make only one further comment: these tests require prime factors of $N - 1$. Later, using linear recurring sequences, other tests will be presented, requiring prime factors of $N + 1$.

IV   Lucas Sequences

Let P, Q be nonzero integers.

Consider the polynomial $X^2 - PX + Q$; its discriminant is $D = P^2 - 4Q$ and the roots are

$$\left.\begin{array}{c}\alpha\\\beta\end{array}\right\} = \frac{P \pm \sqrt{D}}{2}\,.$$

So

$$\begin{cases}\alpha + \beta = P,\\\quad\alpha\beta = Q,\\\alpha - \beta = \sqrt{D}.\end{cases}$$

I shall assume that $D \neq 0$. Note that $D \equiv 0 \pmod 4$ or $D \equiv 1 \pmod 4$. Define the sequences of numbers

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n(P,Q) = \alpha^n + \beta^n, \quad \text{for } n \geq 0.$$

In particular, $U_0(P,Q) = 0$, $U_1(P,Q) = 1$, while $V_0(P,Q) = 2$, $V_1(P,Q) = P$.

The sequences

$$U(P,Q) = (U_n(P,Q))_{n\geq 0} \quad \text{and} \quad V(P,Q) = (V_n(P,Q))_{n\geq 0}$$

are called the *Lucas sequences associated to the pair* (P,Q). Special cases had been considered by Fibonacci, Fermat, and Pell, among others. Many particular facts were known about these sequences; however, the general theory was first developed by Lucas in a seminal paper, which appeared in Volume I of the *American Journal of Mathematics*, 1878. It is a long memoir with a rich content, relating Lucas sequences to many interesting topics, like trigonometric functions, continued fractions, the number of divisions in the algorithm of the greatest common divisor, and also, primality tests. It is for this latter reason that I discuss Lucas sequences. If you are curious about the other connections that I have mentioned, look at the references at the end of the book and/or consult the paper in the library.

I should, however, warn that despite the importance of the paper, the methods employed are often indirect and cumbersome, so it is advisable to read Carmichael's long article of 1913, where he corrected errors and generalized results.

The first thing to note is that, for every $n \geq 2$,

$$\begin{cases} U_n(P,Q) = P\,U_{n-1}(P,Q) - Q\,U_{n-2}(P,Q), \\ V_n(P,Q) = P\,V_{n-1}(P,Q) - Q\,V_{n-2}(P,Q). \end{cases}$$

(just check it). So, these sequences deserve to be called *linear recurring sequences of order* 2 (each term depends linearly on the two preceding terms). Conversely, if P, Q are as indicated, and $D = P^2 - 4Q \neq 0$, if $W_0 = 0$ (resp. 2), $W_1 = 1$ (resp. P), if $W_n = PW_{n-1} - QW_{n-2}$ for $n \geq 2$, then Binet showed (in 1843) that

$$W_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad (\text{resp. } W_n = \alpha^n + \beta^n) \quad \text{for } n \geq 0;$$

here α, β are the roots of the polynomial $X^2 - PX + Q$. This is trivial, because the sequences of numbers

$$(W_n)_{n \geq 0} \quad \text{and} \quad \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right)_{n \geq 0} \quad (\text{resp. } (\alpha^n + \beta^n)_{n \geq 0}),$$

have the first two terms equal and both have the same linear second-order recurrence definition.

Before I continue, here are the main special cases that had been considered before the full theory was developed.

The sequence corresponding to $P = 1$, $Q = -1$, $U_0 = U_0(1,-1) = 0$, and $U_1 = U_1(1,-1) = 1$ was first considered by Fibonacci, and it begins as follows:

$$0, \ 1, \ 1, \ 2, \ 3, \ 5, \ 8, \ 13, \ 21, \ 34, \ 55, \ 89, \ 144, \ 233,$$
$$377, \ 610, \ 987, \ 1597, \ 2584, \ 4181, \ 6765, \ \ldots$$

These numbers appeared for the first time in a problem in Fibonacci's *Liber Abaci*, published in 1202. It was also in this book that Arabic figures were first introduced in Europe. The problem, now reproduced in many elementary books, concerned rabbits having certain reproductive patterns. I do not care for such an explanation. As regards rabbits, I rather prefer to eat a good plate of "lapin chasseur" with fresh noodles.

The companion sequence of Fibonacci numbers, still with $P = 1$, $Q = -1$, is the sequence of Lucas numbers: $V_0 = V_0(1,-1) = 2$,

$V_1 = V_1(1, -1) = 1$, and it begins as follows:

$$2,\ 1,\ 3,\ 4,\ 7,\ 11,\ 18,\ 29,\ 47,\ 76,\ 123,\ 199,\ 322,$$
$$521,\ 843,\ 1364,\ 2207,\ 3571,\ 5778,\ 9349,\ 15127,\ \ldots$$

If $P = 3$, $Q = 2$, then the sequences obtained are

$$U_n(3, 2) = 2^n - 1 \quad \text{and} \quad V_n(3, 2) = 2^n + 1, \quad \text{for } n \geq 0.$$

These sequences were the cause of many sleepness nights for Fermat (see details in Sections VI and VII). The sequences associated to $P = 2$, $Q = -1$, are called the Pell sequences; they begin as follows:

$$U_n(2, -1) :\quad 0,\ 1,\ 2,\ 5,\ 12,\ 29,\ 70,\ 169,\ 408,\ 985,$$
$$2378,\ 5741,\ 13860,\ \ldots$$
$$V_n(2, -1) :\quad 2,\ 2,\ 6,\ 14,\ 34,\ 82,\ 198,\ 478,\ 1154,$$
$$2786,\ 6726,\ 16238,\ 39202,\ \ldots$$

Lucas noted a great similarity between the sequences of numbers $U_n(P, Q)$ (resp. $V_n(P, Q)$) and $(a^n - b^n)/(a - b)$ (resp. $a^n + b^n$), where a, b are given, $a > b \geq 1$, $\gcd(a, b) = 1$ and $n \geq 0$. No wonder, one is a special case of the other. Just observe that for the pair $(a + b, ab)$, $D = (a - b)^2 \neq 0$, $\alpha = a$, $\beta = b$, so

$$U_n(a + b, ab) = \frac{a^n - b^n}{a - b}, \quad V_n(a + b, ab) = a^n + b^n.$$

It is clearly desirable to extend the main results about the sequence of numbers $(a^n - b^n)/(a - b)$, $a^n + b^n$ (in what relates to divisibility and primality) for the wider class of Lucas sequences.

I shall therefore present the generalizations of Fermat's little theorem, Euler's theorem, etc., to Lucas sequences. There is no essential difficulty, but the development requires a surprising number of steps—true enough, all at an elementary level. In what follows, I shall record, one after the other, the facts needed to prove the main results. If you wish, work out the details. But I am also explicitly giving the beginning of several Lucas sequences, so you may be happy just to check my statements numerically (see the tables at the end of the section).

First, the algebraic facts, then the divisibility properties. To simplify the notations, I write only $U_n = U_n(P, Q)$, $V_n = V_n(P, Q)$.

We have the following algebraic properties:

(IV.1) $U_n = PU_{n-1} - QU_{n-2}$ $(n \geq 2)$, $U_0 = 0$, $U_1 = 1$,

$V_n = PV_{n-1} - QV_{n-2}$ $(n \geq 2)$, $V_0 = 2$, $V_1 = P$.

(IV.2) $U_{2n} = U_n V_n$,

$V_{2n} = V_n^2 - 2Q^n$.

(IV.3) $U_{m+n} = U_m V_n - Q^n U_{m-n}$,

$V_{m+n} = V_m V_n - Q^n V_{m-n}$ (for $m \geq n$).

(IV.4) $U_{m+n} = U_m U_{n+1} - QU_{m-1}U_n$,

$2V_{m+n} = V_m V_n + DU_m U_n$.

(IV.5) $DU_n = 2V_{n+1} - PV_n$,

$V_n = 2U_{n+1} - PU_n$.

(IV.6) $U_n^2 = U_{n-1}U_{n+1} + Q^{n-1}$,

$V_n^2 = DU_n^2 + 4Q^n$.

(IV.7) $U_m V_n - U_n V_m = 2Q^n U_{m-n}$ (for $m \geq n$),

$U_m V_n + U_n V_m = 2U_{m+n}$.

(IV.8) $2^{n-1}U_n = \binom{n}{1}P^{n-1} + \binom{n}{3}P^{n-3}D + \binom{n}{5}P^{n-5}D^2 + \cdots$,

$2^{n-1}V_n = P^n + \binom{n}{2}P^{n-2}D + \binom{n}{4}P^{n-4}D^2 + \cdots$.

(IV.9) If m is odd and $k \geq 1$, then

$$D^{(m-1)/2}U_k^m = U_{km} - \binom{m}{1}Q^k U_{k(m-2)} + \binom{m}{2}Q^{2k}U_{k(m-4)} - \cdots$$

$$\pm \binom{m}{(m-1)/2}Q^{\frac{m-1}{2}k}U_k,$$

$$V_k^m = V_{km} + \binom{m}{1}Q^k V_{k(m-2)} + \binom{m}{2}Q^{2k}V_{k(m-4)} + \cdots$$

$$+ \binom{m}{(m-1)/2}Q^{\frac{m-1}{2}k}V_k.$$

If m is even and $k \geq 1$, then

$$D^{m/2}U_k^m = \left[V_{km} - \binom{m}{1}Q^k V_{k(m-2)} + \binom{m}{2}Q^{2k}V_{k(m-4)} - \cdots\right.$$

$$+(-1)^{m/2}\binom{m}{m/2}Q^{(m/2)k}V_0\bigg] - (-1)^{m/2}\binom{m}{m/2}Q^{(m/2)\,k},$$

$$V_k^m = \bigg[V_{km} + \binom{m}{1}Q^k V_{k(m-2)} + \binom{m}{2}Q^{2k}V_{k(m-4)} + \cdots$$

$$+ \binom{m}{m/2}Q^{(m/2)k}V_0\bigg] - \binom{m}{m/2}Q^{(m/2)k}.$$

(IV.10) $U_m = V_{m-1} + QV_{m-3} + Q^2 V_{m-5} + \cdots + \text{(last summand)},$
where

$$\text{last summand} = \begin{cases} Q^{(m-2)/2}\,P & \text{if } m \text{ is even,} \\ Q^{(m-1)/2} & \text{if } m \text{ is odd.} \end{cases}$$

$$P^m = V_m + \binom{m}{1}QV_{m-2} + \binom{m}{2}Q^2 V_{m-4} + \cdots + \text{(last summand)},$$

where

$$\text{last summand} = \begin{cases} \binom{m}{m/2}Q^{m/2} & \text{if } m \text{ is even,} \\ \binom{m}{(m-1)/2}Q^{(m-1)/2}\,P & \text{if } m \text{ is odd.} \end{cases}$$

The following identity of Lagrange, dating from 1741, is required for the next property:

$$X^n + Y^n = (X+Y)^n - \frac{n}{1}XY(X+Y)^{n-2}$$
$$+ \frac{n}{2}\binom{n-3}{1}X^2 Y^2 (X+Y)^{n-4}$$
$$- \frac{n}{3}\binom{n-4}{2}X^3 Y^3 (X+Y)^{n-6} + \cdots$$
$$+ (-1)^r \frac{n}{r}\binom{n-r-1}{r-1}X^r Y^r (X+Y)^{n-2r} \pm \cdots,$$

where the sum is extended for $2r \le n$. Note that each coefficient is an integer.

(IV.11)   If $m \geq 1$ and q is odd,

$$U_{mq} = D^{(q-1)/2}\, U_m^q + \frac{q}{1}\, Q^m D^{(q-3)/2}\, U_m^{q-2}$$

$$+ \frac{q}{2}\binom{q-3}{1} Q^{2m} D^{(q-5)/2}\, U_m^{q-4} + \cdots$$

$$+ \frac{q}{r}\binom{q-r-1}{r-1} Q^{mr} D^{(q-2r-1)/2} U_m^{q-2r} + \cdots$$

$$+ \text{ last summand,}$$

where the last summand is

$$\frac{q}{(q-1)/2}\binom{(q-1)/2}{(q-3)/2} Q^{\frac{q-1}{2}m}\, U_m = q\, Q^{\frac{q-1}{2}m}\, U_m.$$

Now, I begin to indicate, one after the other, the divisibility properties, in the order in which they may be proved.

(IV.12) $U_n \equiv V_{n-1} \pmod{Q},$

$$V_n \equiv P^n \pmod{Q}.$$

Hint: Use (IV.10) or proceed by induction.

(IV.13)   Let p be an odd prime, then

$$U_{kp} \equiv D^{\frac{p-1}{2}} U_k \pmod{p}$$

and, for $e \geq 1$,

$$U_{p^e} \equiv D^{\frac{p-1}{2}e} \pmod{p}.$$

In particular,

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}.$$

Hint: Use (IV.9).

(IV.14) $V_p \equiv P \pmod{p}.$

Hint: Use (IV.10).

(IV.15)   If $n, k \geq 1$, then U_n divides U_{kn}.

Hint: Use (IV.3).

(IV.16)   If $n, k \geq 1$ and k is odd, then V_n divides V_{kn}.

Hint: Use (IV.9).

Notation. If $n \geq 2$ and if there exists $r \geq 1$ such that n divides U_r, denote by $\rho(n) = \rho(n, U)$ the smallest such r.

(IV.17)   Assume that $\rho(n)$ exists and $\gcd(n, 2Q) = 1$. Then $n \mid U_k$ if and only if $\rho(n) \mid k$.

Hint: Use (IV.15) and (IV.7).

   It will be seen that $\rho(n)$ exists, for many—not for all—values of n, such that $\gcd(n, 2Q) = 1$.

(IV.18)   If Q is even and P is even, then U_n is even (for $n \geq 2$) and V_n is even (for $n \geq 1$).
   If Q is even and P is odd, then U_n, V_n are odd (for $n \geq 1$).
   If Q is odd and P is even, then $U_n \equiv n \pmod{2}$ and V_n is even.
   If Q is odd and P is odd, then U_n, V_n are even if 3 divides n, while U_n, V_n are odd, otherwise.
   In particular, if U_n is even, then V_n is even.

Hint: Use (IV.12), (IV.5), (IV.2), (IV.6), and (IV.1).

   Here is the first main result, which is a companion of (IV.18) and generalizes Fermat's little theorem:

(IV.19)   Let p be an odd prime.
   If $p \mid P$ and $p \mid Q$, then $p \mid U_k$ for every $k > 1$.
   If $p \mid P$ and $p \nmid Q$, then $p \mid U_k$ exactly when k is even.
   If $p \nmid P$ and $p \mid Q$, then $p \nmid U_k$ for every $k \geq 1$.
   If $p \nmid P$, $p \nmid Q$, and $p \mid D$, then $p \mid U_k$ exactly when $p \mid k$.
   If $p \nmid PQD$, then $p \mid U_{\psi(p)}$, where $\psi(p) = p - (D \mid p)$, and $(D \mid p)$ denotes the Legendre symbol.

Proof. If $p \mid P$ and $p \mid Q$, by (IV.1) $p \mid U_k$ for every $k > 1$.
   If $p \mid P = U_2$, by (IV.15) $p \mid U_{2k}$ for every $k \geq 1$. Since $p \nmid Q$, and $U_{2k+1} = PU_{2k} - QU_{2k-1}$, by induction, $p \nmid U_{2k+1}$.
   If $p \nmid P$ and $p \mid Q$, by induction and (IV.1), $p \nmid U_k$ for every $k \geq 1$.
   If $p \nmid PQ$ and $p \mid D$, by (IV.8), $2^{p-1}U_p \equiv 0 \pmod{p}$ so $p \mid U_p$. On the other hand, if $p \nmid n$, then by (IV.8), $2^{n-1}U_n \equiv nP^{n-1} \not\equiv 0 \pmod{p}$, so $p \nmid U_n$.

Finally the more interesting case: assume $p \nmid PQD$.
If $(D \mid p) = -1$, then by (IV.8)

$$2^p U_{p+1} = \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2}D + \cdots$$
$$+ \binom{p+1}{p} PD^{(p-1)/2} \equiv P + PD^{(p-1)/2} \equiv 0 \pmod{p},$$

so $p \mid U_{p+1}$.

If $(D \mid p) = 1$, there exists C such that $P^2 - 4Q = D \equiv C^2$ (mod p); hence, $P^2 \not\equiv C^2 \pmod{p}$ and $p \nmid C$. By (IV.8), noting that

$$\binom{p-1}{1} \equiv -1 \pmod{p}, \quad \binom{p-1}{3} \equiv -1 \pmod{p}, \quad \dots$$

we see that

$$2^{p-2} U_{p-1} = \binom{p-1}{1} P^{p-2} + \binom{p-1}{3} P^{p-4}D$$
$$+ \binom{p-1}{5} P^{p-6}D^2 + \cdots + \binom{p-1}{p-2} PD^{(p-3)/2}$$
$$\equiv -[P^{p-2} + P^{p-4}D + P^{p-6}D^2 + \cdots + PD^{(p-3)/2}]$$
$$\equiv -P\left(\frac{P^{p-1} - D^{(p-1)/2}}{P^2 - D}\right)$$
$$\equiv -P\frac{P^{p-1} - C^{p-1}}{P^2 - C^2} \equiv 0 \pmod{p}.$$

So $p \mid U_{p-1}$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

If I want to use the notation $\rho(p)$ introduced before, some of the assertions of (IV.19) may be restated as follows:

If p is an odd prime and $p \nmid Q$, then:
If $p \mid P$, then $\rho(p) = 2$.
If $p \nmid P$, $p \mid D$, then $\rho(p) = p$.
If $p \nmid PD$, then $\rho(p)$ divides $\psi(p)$.

Don't conclude hastily that, in this latter case, $\rho(p) = \psi(p)$. I shall return to this point, after I list the main properties of the Lucas sequences.

For the special Lucas sequence $U_n(a+1, a)$, the discriminant is $D = (a-1)^2$; so if $p \nmid a(a^2 - 1)$, then

$$\left(\frac{D}{p}\right) = 1 \qquad \text{and} \qquad p \mid U_{p-1} = \frac{a^{p-1} - 1}{a - 1},$$

so $p \mid a^{p-1} - 1$ (this is trivial if $p \mid a^2 - 1$)—which is Fermat's little theorem.

(IV.20)   Let $e \geq 1$, and let p^e be the exact power of p dividing U_m. If $p \nmid k$ and $f \geq 1$, then p^{e+f} divides U_{mkp^f}.

Moreover, if $p \mid Q$ and $p^e \neq 2$, then p^{e+f} is the exact power of p dividing U_{mkp^f}, while if $p^e = 2$ then $U_{mk}/2$ is odd.

Hint: Use (IV.19), (IV.18), (IV.11), and (IV.6).

And now the generalization of Euler's theorem:

If α, β are roots of $X^2 - PX + Q$, define the symbol:

$$\left(\frac{\alpha, \beta}{2}\right) = \begin{cases} 1 & \text{if } Q \text{ is even,} \\ 0 & \text{if } Q \text{ is odd, } P \text{ even,} \\ -1 & \text{if } Q \text{ is odd, } P \text{ odd} \end{cases}$$

and for $p \neq 2$:

$$\left(\frac{\alpha, \beta}{p}\right) = \left(\frac{D}{p}\right)$$

(so it is 0 if $p \mid D$). Put

$$\psi_{\alpha,\beta}(p) = p - \left(\frac{\alpha, \beta}{p}\right)$$

for every prime p, also

$$\psi_{\alpha,\beta}(p^e) = p^{e-1}\psi_{\alpha,\beta}(p) \quad \text{for } e \geq 1.$$

If $n = \prod_{p|n} p^e$, define the Carmichael function

$$\lambda_{\alpha,\beta}(n) = \operatorname{lcm}\{\psi_{\alpha,\beta}(p^e)\}$$

(where lcm denotes the least common multiple), and define the generalized Euler function

$$\psi_{\alpha,\beta}(n) = \prod_{p|n} \psi_{\alpha,\beta}(p^e).$$

So $\lambda_{\alpha,\beta}(n)$ divides $\psi_{\alpha,\beta}(n)$.

It is easy to check that $\psi_{a,1}(p) = p-1 = \varphi(p)$ for every prime p not dividing a; so if $\gcd(a,n) = 1$, then $\psi_{a,1}(n) = \varphi(n)$ and also $\lambda_{a,1}(n) = \lambda(n)$, where $\lambda(n)$ is the function, also defined by Carmichael, and considered in Section II.

And here is the extension of Euler's theorem:

(IV.21)   If $\gcd(n,Q) = 1$, then n divides $U_{\lambda_{\alpha,\beta}(n)}$; hence, also n divides $U_{\psi_{\alpha,\beta}(n)}$.

Hint: Use (IV.19) and (IV.20).

It should be said that the divisibility properties of the companion sequence $(V_n)_{n \geq 1}$ are not so simple to describe. Note, for example,

(IV.22)   If $p \nmid 2QD$, then $V_{p-(D|p)} \equiv 2Q^{\frac{1}{2}[1-(D|p)]} \pmod{p}$.

Hint: Use (IV.5), (IV.13), (IV.19), and (IV.14).

This may be applied to give divisibility results for $U_{\psi(p)/2}$ and $V_{\psi(p)/2}$.

(IV.23)   Assume that $p \nmid 2QD$. Then

$$p \mid U_{\psi(p)/2} \quad \text{if and only if} \quad (Q \mid p) = 1,$$
$$p \mid V_{\psi(p)/2} \quad \text{if and only if} \quad (Q \mid p) = -1.$$

Hint: For the first assertion, use (IV.2), (IV.6), (IV.22) and the congruence $(Q \mid p) \equiv Q^{(p-1)/2} \pmod{p}$. For the second assertion, use (IV.2), (IV.19), the first assertion, and also (IV.6).

For the next results, I shall assume that $\gcd(P,Q) = 1$.

(IV.24) $\gcd(U_n, Q) = 1$ and $\gcd(V_n, Q) = 1$, for every $n \geq 1$.

Hint: Use (IV.12).

(IV.25) $\gcd(U_n, V_n) = 1$ or 2.

Hint: Use (IV.16) and (IV.24).

(IV.26)   If $d = \gcd(m,n)$, then $U_d = \gcd(U_m, U_n)$.

Hint: Use (IV.15), (IV.7), (IV.24), (IV.18), and (IV.6). This proof is actually not so easy, and requires the use of the Lucas sequence $\big(U_n(V_d, Q^d)\big)_{n \geq 0}$.

(IV.27)   If $\gcd(m, n) = 1$, then $\gcd(U_m, U_n) = 1$.

No hint for this one.

(IV.28)   If $d = \gcd(m, n)$ and m/d, n/d are odd, then
$$V_d = \gcd(V_m, V_n).$$

Hint: Use the same proof as for (IV.26).

And here is a result similar to (IV.17), but with the assumption that $\gcd(P, Q) = 1$:

(IV.29)   Assume that $\rho(n)$ exists. Then $n \mid U_k$ if and only if $\rho(n) \mid k$.

Hint: Use (IV.15), (IV.24), and (IV.3).

I pause to write explicitly what happens for the Fibonacci numbers U_n and Lucas numbers V_n; now $P = 1$, $Q = -1$, $D = 5$.

Property (IV.18) becomes the *law of appearance* of p; even though I am writing this text on Halloween's evening, it would hurt me to call it the "apparition law" (as it was badly translated from the French *loi d'apparition*; in all English dictionaries "apparition" means "ghost"). Law of apparition (oops!, appearance) of p:

$$p \mid U_{p-1} \text{ if } (5 \mid p) = 1, \quad \text{that is, } p \equiv \pm 1 \ (\text{mod } 10),$$
$$p \mid U_{p+1} \text{ if } (5 \mid p) = -1, \text{ that is, } p \equiv \pm 3 \ (\text{mod } 10).$$

Property (IV.19) is the *law of repetition*.

For the Lucas numbers, the following properties hold:

$$p \mid V_{p-1} - 2 \text{ if } (5 \mid p) = 1, \quad \text{that is, } p \equiv \pm 1 \ (\text{mod } 10),$$
$$p \mid V_{p+1} + 2 \text{ if } (5 \mid p) = -1, \text{ that is, } p \equiv \pm 3 \ (\text{mod } 10).$$

Jarden showed in 1958 that, for the Fibonacci sequence, the function
$$\frac{\psi(p)}{\rho(p)} = \frac{p - (5 \mid p)}{\rho(p)}$$
is unbounded (when the prime p tends to infinity).

This result was generalized by Kiss & Phong in 1978: there exists $C > 0$ (depending only on P, Q) such that $\psi(p)/\rho(p)$ is unbounded, but still $\psi(p)/\rho(p) < C[p/(\log p)]$ (when the prime p tends to infinity).

Now I shall indicate the behaviour of Lucas sequences modulo a prime p.

If $p = 2$, this is as described in (IV.18). For example, if P, Q are odd, then the sequences $(U_n \bmod 2)_{n \geq 0}$, $(V_n \bmod 2)_{n \geq 0}$ are equal to

$$0, \ 1, \ 1, \ 0, \ 1, \ 1, \ 0, \ 1, \ 1, \ 0, \ \ldots \ .$$

It is more interesting when p is an odd prime.

(IV.30)   If $p \nmid 2QD$ and $(D \mid p) = 1$, then

$$U_{n+p-1} \equiv U_n \quad (\bmod \ p),$$
$$V_{n+p-1} \equiv V_n \quad (\bmod \ p).$$

Thus, the sequences $(U_n \bmod p)_{n \geq 0}$, $(V_n \bmod p)_{n \geq 0}$ have period $p-1$.

Proof. By (IV.4), $U_{n+p-1} = U_n U_p - QU_{n-1}U_{p-1}$; by (IV.19), $\rho(p)$ divides $p - (D \mid p) = p - 1$; by (IV.15), $p \mid U_{p-1}$; this is also true if $p \mid P$, $p \nmid Q$, because then $p - 1$ is even, so $p \mid U_{p-1}$, by (IV.19). By (IV.13),
$$U_p \equiv (D \mid p) \equiv 1 \quad (\bmod \ p).$$
So $U_{n+p-1} \equiv U_n \ (\bmod \ p)$.

Now, by (IV.5), $V_{n+p-1} = 2U_{n+p} - PU_n \equiv 2U_{n+1} - PU_n \equiv V_n$ $(\bmod \ p)$.   □

The companion result is the following:

(IV.31)   Let $p \nmid 2QD$, let e be the order of Q mod p. If $(D \mid p) = -1$, then

$$U_{n+e(p+1)} \equiv U_n \quad (\bmod \ p),$$
$$V_{n+e(p+1)} \equiv V_n \quad (\bmod \ p).$$

Thus, the sequences $(U_n \bmod p)_{n \geq 0}$, $(V_n \bmod p)_{n \geq 0}$ have period $e(p + 1)$.

Proof. If $p \nmid P$, then by (IV.19), (IV.15),

$$p \mid U_{p-(D|p)} = U_{p+1} \, .$$

This is also true when $p \mid P$.

By (IV.22), $V_{p+1} \equiv 2Q \pmod{p}$. Now I show, by induction on $r \geq 1$, that $V_{r(p+1)} \equiv 2Q^r \pmod{p}$.

If this is true for $r \geq 1$, then by (IV.4)

$$2V_{(r+1)(p+1)} = V_{r(p+1)}V_{p+1} + DU_{r(p+1)}U_{p+1} \equiv 4Q^{r+1} \pmod{p},$$

so $V_{(r+1)(p+1)} \equiv 2Q^{r+1} \pmod{p}$. In particular, $V_{e(p+1)} \equiv 2Q^e \equiv 2 \pmod{p}$. By (IV.7),

$$U_{n+e(p+1)}V_{e(p+1)} - U_{e(p+1)}V_{n+e(p+1)} = 2Q^{e(p+1)} U_n \, ,$$

hence $2U_{n+e(p+1)} \equiv 2U_n \pmod{p}$ and the first congruence is established.

The second congruence follows using (IV.5).   □

It is good to summarize some of the preceding results, in terms of the sets

$$\mathcal{P}(U) = \{p \text{ prime} \mid \text{there exists } n \text{ such that } U_n \neq 0 \text{ and } p \mid U_n\},$$
$$\mathcal{P}(V) = \{p \text{ prime} \mid \text{there exists } n \text{ such that } V_n \neq 0 \text{ and } p \mid V_n\}.$$

These are the sets of prime divisors of the sequences $U = (U_n)_{n \geq 1}$ and $V = (V_n)_{n \geq 1}$, respectively.

The parameters (P, Q) are assumed to be nonzero, relatively prime integers and the discriminant is $D = P^2 - 4Q \neq 0$.

A first case arises if there exists $n > 1$ such that $U_n = 0$; equivalently, $\alpha^n = \beta^n$, that is α/β is a root of unity. If n is the smallest such index, then $U_r \neq 0$ for $r = 1, \dots, n-1$ and $U_{nk+r} = \alpha^{nk}U_r$ (for every $k \geq 1$), so $\mathcal{P}(U)$ consists of the prime divisors of $U_2 \cdots U_{n-1}$. Similarly, $\mathcal{P}(V)$ consists of the prime numbers dividing $V_1 V_2 \cdots V_{n-1}V_n$.

The more interesting case is when α/β is not a root of unity, so $U_n \neq 0$, $V_n \neq 0$, for every $n \geq 1$. Then $\mathcal{P}(U) = \{p \text{ prime} \mid p \text{ does not divide } Q\}$.

This follows from (IV.18) and (IV.19). In particular, for the sequence of Fibonacci numbers, $\mathcal{P}(U)$ is the set of all primes.

Nothing so precise may be said about the companion Lucas sequence $V = (V_n)_{n \geq 1}$. From $U_{2n} = U_n V_n$ ($n \geq 1$) it follows that $\mathcal{P}(V)$

is a subset of $\mathcal{P}(U)$. From (IV.18), $2 \in \mathcal{P}(V)$ if and only if Q is odd. Also, from (IV.24) and (IV.6), if $p \neq 2$ and if $p \mid DQ$, then $p \notin \mathcal{P}(V)$, while if $p \nmid 2DQ$ and $(Q \mid p) = -1$, then $p \in \mathcal{P}(V)$ [see (IV.23)]; on the other hand, if $p \nmid 2DQ$, $(Q \mid p) = 1$, and $(D \mid p) = -(-1 \mid p)$, then $p \notin \mathcal{P}(V)$. This does not determine, without a further analysis, whether a prime p, such that $p \nmid 2DQ$, $(Q \mid p) = 1$, and $(D \mid p) = (-1 \mid p)$ belongs, or does not belong, to $\mathcal{P}(V)$. At any rate, it shows that $\mathcal{P}(V)$ is also an infinite set.

For the sequence of Lucas numbers, with $P = 1$, $Q = -1$, $D = 5$, the preceding facts may be explicitly stated as follows:

if $p = 3, 7, 11, 19 \pmod{20}$, then $p \in \mathcal{P}(V)$;

if $p \equiv 13, 17 \pmod{20}$, then $p \notin \mathcal{P}(V)$.

For $p \equiv 1, 9 \pmod{20}$, no decision may be obtained without a careful study, as, for example, that done by Ward in 1961. Already in 1958 Jarden had shown that there exist infinitely many primes p, $p \equiv 1 \pmod{20}$, such that $p \notin \mathcal{P}(V)$, and, on the other hand, there exist also infinitely many primes p, $p \equiv 1 \pmod{40}$, such that $p \in \mathcal{P}(V)$.

Later, in Chapter 5, Section VIII, I shall return to the study of the sets $\mathcal{P}(U)$, $\mathcal{P}(V)$, asking for their density in the set of all primes.

In analogy with the theorem of Bang and Zsigmondy, Carmichael also considered the primitive prime factors of the Lucas sequences, with parameters (P, Q): p is a primitive prime factor of U_k (resp. V_k) if $p \mid U_k$ (resp. $p \mid V_k$), but p does not divide any preceding number in the sequence in question.

The proof of Zsigmondy's theorem is not too simple; here it is somewhat more delicate.

Carmichael showed that if the discriminant D is positive, then for every $n \neq 1, 2, 6$, U_n has a primitive prime factor, except if $n = 12$ and $P = \pm 1$, $Q = -1$.

Moreover, if D is a square, then it is better: for every n, U_n has a primitive prime factor, except if $n = 6$, $P = \pm 3$, $Q = 2$.

Do you recognize that this second statement includes Zsigmondy's theorem? Also, if $P = 1$, $Q = -1$ the exception is the Fibonacci number $U_{12} = 144$.

For the companion sequence, if $D > 0$, then for every $n \neq 1, 3$, V_n has a primitive prime factor, except if $n = 6$, $P = \pm 1$, $Q = -1$ (the Lucas number $V_6 = 18$). Moreover, if D is a square, then the only

exception is $n = 3$, $P = \pm 3$, $Q = 2$, also contained in Zsigmondy's theorem.

If, however, $D < 0$, the result indicated is no longer true. Thus, as Carmichael already noted, if $P = 1$, $Q = 2$, then for $n = 1, 2, 3, 5, 8, 12, 13, 18$, U_n has no primitive prime factors.

Schinzel showed the following in 1962:

Let $(U_n)_{n \geq 0}$ be the Lucas sequence with relatively prime parameters (P, Q) and assume that the discriminant is $D < 0$. Assume that α/β is not a root of unity. Then there exists n_0 (depending on P, Q), effectively computable, such that if $n > n_0$, then U_n has a primitive prime factor.

Later, in 1974, Schinzel proved the same result with an absolute constant n_0—independent of the Lucas sequence. This was a remarkable result.

Making use of the methods of Baker, Stewart determined in 1977 that if $n > e^{452} 2^{67}$, then U_n has a primitive prime factor. Moreover, Stewart also showed that if n is given ($n \neq 6$, $n > 4$), there are only finitely many Lucas sequences, which may be determined explicitly (so says Stewart, without doing it), for which U_n has no primitive prime factor.

It is interesting to consider the primitive part U_n^* of U_n:

$$U_n = U_n^* U_n' \quad \text{with} \quad \gcd(U_n^*, U_n') = 1$$

and p divides U_n^* if and only if p is a primitive prime factor of U_n.

In 1963, Schinzel indicated conditions for the existence of two (or even $e > 2$) distinct primitive prime factors. It follows that if $D > 0$ or $D < 0$ and α/β is not a root of unity, there exist infinitely many n such that the primitive part U_n^* is composite.

Can one say anything about U_n^* being square-free? This is a very deep question. Just think of the special case when $P = 3$, $Q = 2$, which gives the sequence $2^n - 1$ (see my comments in Section II).

Table 2.   Fibonacci and Lucas numbers

$$P = 1, \ Q = -1$$

Fibonacci numbers	Lucas numbers
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 1$
$U(2) = 1$	$V(2) = 3$
$U(3) = 2$	$V(3) = 4$
$U(4) = 3$	$V(4) = 7$
$U(5) = 5$	$V(5) = 11$
$U(6) = 8$	$V(6) = 18$
$U(7) = 13$	$V(7) = 29$
$U(8) = 21$	$V(8) = 47$
$U(9) = 34$	$V(9) = 76$
$U(10) = 55$	$V(10) = 123$
$U(11) = 89$	$V(11) = 199$
$U(12) = 144$	$V(12) = 322$
$U(13) = 233$	$V(13) = 521$
$U(14) = 377$	$V(14) = 843$
$U(15) = 610$	$V(15) = 1364$
$U(16) = 987$	$V(16) = 2207$
$U(17) = 1597$	$V(17) = 3571$
$U(18) = 2584$	$V(18) = 5778$
$U(19) = 4181$	$V(19) = 9349$
$U(20) = 6765$	$V(20) = 15127$
$U(21) = 10946$	$V(21) = 24476$
$U(22) = 17711$	$V(22) = 39603$
$U(23) = 28657$	$V(23) = 64079$
$U(24) = 46368$	$V(24) = 103682$
$U(25) = 75025$	$V(25) = 167761$
$U(26) = 121393$	$V(26) = 271443$
$U(27) = 196418$	$V(27) = 439204$
$U(28) = 317811$	$V(28) = 710647$
$U(29) = 514229$	$V(29) = 1149851$
$U(30) = 832040$	$V(30) = 1860498$
$U(31) = 1346269$	$V(31) = 3010349$
$U(32) = 2178309$	$V(32) = 4870847$
$U(33) = 3524578$	$V(33) = 7881196$
$U(34) = 5702887$	$V(34) = 12752043$
$U(35) = 9227465$	$V(35) = 20633239$
$U(36) = 14930352$	$V(36) = 33385282$
$U(37) = 24157817$	$V(37) = 54018521$
$U(38) = 39088169$	$V(38) = 87403803$
$U(39) = 63245986$	$V(39) = 141422324$
$U(40) = 102334155$	$V(40) = 228826127$

Table 3.   Numbers $2^n - 1$ and $2^n + 1$

$$P = 3, \ Q = 2$$

Numbers $2^n - 1$	Numbers $2^n + 1$
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 3$
$U(2) = 3$	$V(2) = 5$
$U(3) = 7$	$V(3) = 9$
$U(4) = 15$	$V(4) = 17$
$U(5) = 31$	$V(5) = 33$
$U(6) = 63$	$V(6) = 65$
$U(7) = 127$	$V(7) = 129$
$U(8) = 255$	$V(8) = 257$
$U(9) = 511$	$V(9) = 513$
$U(10) = 1023$	$V(10) = 1025$
$U(11) = 2047$	$V(11) = 2049$
$U(12) = 4095$	$V(12) = 4097$
$U(13) = 8191$	$V(13) = 8193$
$U(14) = 16383$	$V(14) = 16385$
$U(15) = 32767$	$V(15) = 32769$
$U(16) = 65535$	$V(16) = 65537$
$U(17) = 131071$	$V(17) = 131073$
$U(18) = 262143$	$V(18) = 262145$
$U(19) = 524287$	$V(19) = 524289$
$U(20) = 1048575$	$V(20) = 1048577$
$U(21) = 2097151$	$V(21) = 2097153$
$U(22) = 4194303$	$V(22) = 4194305$
$U(23) = 8388607$	$V(23) = 8388609$
$U(24) = 16777215$	$V(24) = 16777217$
$U(25) = 33554431$	$V(25) = 33554433$
$U(26) = 67108863$	$V(26) = 67108865$
$U(27) = 134217727$	$V(27) = 134217729$
$U(28) = 268435455$	$V(28) = 268435457$
$U(29) = 536870911$	$V(29) = 536870913$
$U(30) = 1073741823$	$V(30) = 1073741825$
$U(31) = 2147483647$	$V(31) = 2147483649$
$U(32) = 4294967295$	$V(32) = 4294967297$
$U(33) = 8589934591$	$V(33) = 8589934593$
$U(34) = 17179869183$	$V(34) = 17179869185$
$U(35) = 34359738367$	$V(35) = 34359738369$
$U(36) = 68719476735$	$V(36) = 68719476737$
$U(37) = 137438953471$	$V(37) = 137438953473$
$U(38) = 274877906943$	$V(38) = 274877906945$
$U(39) = 549755813887$	$V(39) = 549755813889$
$U(40) = 1099511627775$	$V(40) = 1099511627777$

Table 4.   Pell numbers

$$P = 2, \ Q = -1$$

Pell numbers	Companion Pell numbers
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 2$
$U(2) = 2$	$V(2) = 6$
$U(3) = 5$	$V(3) = 14$
$U(4) = 12$	$V(4) = 34$
$U(5) = 29$	$V(5) = 82$
$U(6) = 70$	$V(6) = 198$
$U(7) = 169$	$V(7) = 478$
$U(8) = 408$	$V(8) = 1154$
$U(9) = 985$	$V(9) = 2786$
$U(10) = 2378$	$V(10) = 6726$
$U(11) = 5741$	$V(11) = 16238$
$U(12) = 13860$	$V(12) = 39202$
$U(13) = 33461$	$V(13) = 94642$
$U(14) = 80782$	$V(14) = 228486$
$U(15) = 195025$	$V(15) = 551614$
$U(16) = 470832$	$V(16) = 1331714$
$U(17) = 1136689$	$V(17) = 3215042$
$U(18) = 2744210$	$V(18) = 7761798$
$U(19) = 6625109$	$V(19) = 18738638$
$U(20) = 15994428$	$V(20) = 45239074$
$U(21) = 38613965$	$V(21) = 109216786$
$U(22) = 93222358$	$V(22) = 263672646$
$U(23) = 225058681$	$V(23) = 636562078$
$U(24) = 543339720$	$V(24) = 1536796802$
$U(25) = 1311738121$	$V(25) = 3710155682$
$U(26) = 3166815962$	$V(26) = 8957108166$
$U(27) = 7645370045$	$V(27) = 21624372014$
$U(28) = 1845756052$	$V(28) = 52205852194$
$U(29) = 44560482149$	$V(29) = 126036076402$
$U(30) = 107578520350$	$V(30) = 304278004998$
$U(31) = 259717522849$	$V(31) = 734592086398$
$U(32) = 627013566048$	$V(32) = 1773462177794$
$U(33) = 1513744654945$	$V(33) = 4281516441986$
$U(34) = 3654502875938$	$V(34) = 10336495061766$
$U(35) = 8822750406821$	$V(35) = 24954506565518$
$U(36) = 21300003689580$	$V(36) = 60245508192802$
$U(37) = 51422757785981$	$V(37) = 145445522951122$
$U(38) = 124145519261542$	$V(38) = 351136554095046$
$U(39) = 299713796309065$	$V(39) = 847718631141214$
$U(40) = 723573111879672$	$V(40) = 2046573816377474$

Table 5.   Numbers $U(4,3)$ and $V(4,3)$

$P = 4, \; Q = 3$

Numbers	Companion numbers
$U(0) = 0 \quad U(1) = 1$	$V(0) = 2 \quad V(1) = 4$
$U(2) = 4$	$V(2) = 10$
$U(3) = 13$	$V(3) = 28$
$U(4) = 40$	$V(4) = 82$
$U(5) = 121$	$V(5) = 244$
$U(6) = 364$	$V(6) = 730$
$U(7) = 1093$	$V(7) = 2188$
$U(8) = 3280$	$V(8) = 6562$
$U(9) = 9841$	$V(9) = 19684$
$U(10) = 29524$	$V(10) = 59050$
$U(11) = 88573$	$V(11) = 177148$
$U(12) = 265720$	$V(12) = 531442$
$U(13) = 797161$	$V(13) = 1594324$
$U(14) = 2391484$	$V(14) = 4782970$
$U(15) = 7174453$	$V(15) = 14348908$
$U(16) = 21523360$	$V(16) = 43046722$
$U(17) = 64570081$	$V(17) = 129140164$
$U(18) = 193710244$	$V(18) = 387420490$
$U(19) = 581130733$	$V(19) = 1162261468$
$U(20) = 1743392200$	$V(20) = 3486784402$
$U(21) = 5230176601$	$V(21) = 10460353204$
$U(22) = 15690529804$	$V(22) = 31381059610$
$U(23) = 47071589413$	$V(23) = 94143178828$
$U(24) = 141214768240$	$V(24) = 282429536482$
$U(25) = 423644304721$	$V(25) = 847288609444$
$U(26) = 1270932914164$	$V(26) = 2541865828330$
$U(27) = 3812798742493$	$V(27) = 7625597484988$
$U(28) = 11438396227480$	$V(28) = 22876792454962$
$U(29) = 34315188682441$	$V(29) = 68630377364884$
$U(30) = 102945566047324$	$V(30) = 205891132094650$
$U(31) = 308836698141973$	$V(31) = 617673396283948$
$U(32) = 926510094425920$	$V(32) = 1853020188851842$
$U(33) = 2779530283277761$	$V(33) = 5559060566555524$
$U(34) = 8338590849833284$	$V(34) = 16677181699666570$
$U(35) = 25015772549499853$	$V(35) = 50031545098999708$
$U(36) = 75047317648499560$	$V(36) = 150094635296999122$
$U(37) = 225141952945498681$	$V(37) = 450283905890997364$
$U(38) = 675425858836496044$	$V(38) = 1350851717672992090$
$U(39) = 2026277576509488133$	$V(39) = 4052555153018976268$
$U(40) = 6078832729528464400$	$V(40) = 12157665459056928802$

V   Primality Tests Based on Lucas Sequences

Lucas began, Lehmer continued, others refined. The primality tests of N, to be presented now, require the knowledge of prime factors of $N+1$, and they complement the tests indicated in Section III, which needed the prime factors of $N-1$. Now, the tool will be the Lucas sequences. By (IV.18), if N is an odd prime, if $U = (U_n)_{n \geq 0}$ is a Lucas sequence with discriminant D and $N \nmid DPQ$, then N divides $U_{N-(D|N)}$. So, if the Jacobi symbol $(D \mid N) = -1$, then N divides U_{N+1}.

However, I note right away (as I did in Section III) that a crude converse does not hold, because there exist composite integers N, and Lucas sequences $(U_n)_{n \geq 0}$ with discriminant D, such that N divides $U_{N-(D|N)}$. Such numbers will be studied in Section X.

It will be convenient to introduce for every integer $D > 1$ the function ψ_D, defined as follows:

If $N = \prod_{i=1}^{s} p_i^{e_i}$, let

$$\psi_D(N) = \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i - 1} \left(p_i - \left(\frac{D}{p_i} \right) \right).$$

Note that if $(U_n)_{n \geq 0}$ is a Lucas sequence with discriminant D, if α, β are the roots of the associated polynomial, then the function $\psi_{\alpha, \beta}$ considered in Section IV is related to ψ_D as follows:

$$\psi_{\alpha, \beta}(N) = 2^{s-1} \psi_D(N).$$

As it will be necessary to consider simultaneously several Lucas sequences with the same discriminant D, it is preferable to work with ψ_D, and not with the functions $\psi_{\alpha, \beta}$ corresponding to the various sequences.

Note, for example, that if $U(P, Q)$ has discriminant D, if $P' = P + 2$, $Q' = P + Q + 1$, then also $U(P', Q')$ has discriminant D.

It is good to start with some preparatory and easy results.

(V.1)   If N is odd, $\gcd(N, D) = 1$, then $\psi_D(N) = N - (D \mid N)$ if and only if N is a prime.

Proof. If N is a prime, by definition $\psi_D(N) = N - (D \mid N)$. If $N = p^e$ with p prime, $e \geq 2$, then $\psi_D(N)$ is a multiple of p, while $N = (D \mid N)$ is not.

If $N = \prod_{i=1}^{s} p_i^{e_i}$, with $s \geq 2$, then

$$\psi_D(N) \leq \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i-1}(p_i + 1) = 2N \prod_{i=1}^{s} \frac{1}{2}\left(1 + \frac{1}{p_i}\right)$$

$$\leq 2N \times \frac{2}{3} \times \frac{3}{5} \times \cdots \leq \frac{4N}{5} < N - 1,$$

since $N > 5$. $\qquad\square$

(V.2)   If N is odd, $\gcd(N, D) = 1$, and $N - (D \mid N)$ divides $\psi_D(N)$, then N is a prime.

Proof. Assume that N is composite. First, let $N = p^e$, with p prime, $e \geq 2$; then $\psi_D(N) = p^e - p^{e-1}(D \mid p)$. Hence,

$$p^e - p^{e-1} < p^e - 1 \leq N - (D \mid N) \leq \psi_D(N) = p^e - p^{e-1}(D \mid p),$$

so $(D \mid p) = -1$ and $N - (D \mid N) = p^e \pm 1$ divides $\psi_D(N) = p^e + p^{e-1} = p^e \pm 1 + (p^{e-1} \mp 1)$, which is impossible.

If N has at least two distinct prime factors, it was seen in (V.1) that $\psi_D(N) < N - 1 \leq N - (D \mid N)$, which is contrary to the hypothesis. So N must be a prime. $\qquad\square$

(V.3)   If N is odd, $U = U(P, Q)$ is a Lucas sequence with discriminant D, and $\gcd(N, QD) = 1$, then $N \mid U_{\psi_D(N)}$.

Proof. Since $\gcd(N, Q) = 1$, then by (IV.12), N divides $\lambda_{\alpha,\beta}(N)$, where α, β are the roots of $X^2 - PX + Q$. If $N = \prod_{i=1}^{s} p_i^{e_i}$, then

$$\lambda_{\alpha,\beta}(N) = \gcd\left\{ p_i^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right) \right\}$$

$$= 2\gcd\left\{ \frac{1}{2} p_i^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right) \right\}$$

and $\lambda_{\alpha,\beta}(N)$ divides

$$2 \prod_{i=1}^{s} \frac{1}{2} p_i^{e_i-1}\left(p_i - \left(\frac{D}{p_i}\right)\right) = \psi_D(N).$$

By (IV.15), N divides $U_{\psi_D(N)}$. $\qquad\square$

(V.4)   If N is odd, $U = U(P,Q)$ is a Lucas sequence with discriminant D such that $(D \mid N) = -1$, and N divides U_{N+1}, then $\gcd(N, QD) = 1$.

Proof. Since $(D \mid N) \neq 0$, then $\gcd(N, D) = 1$. If there exists a prime p such that $p \mid N$ and $p \mid Q$, since $p \nmid D = P^2 - 4Q$, then $p \nmid P$. By (IV.18) $p \nmid U_n$ for every $n \geq 1$, which is contrary to the hypothesis. So $\gcd(N, Q) = 1$. $\qquad\square$

One more result which will be needed is the following:

(V.5)   Let N be odd and q be any prime factor of $N + 1$. Assume that $U = U(P,Q)$ and $V = V(P,Q)$ are the Lucas sequences associated with the integers P, Q, having discriminant $D \neq 0$. Assume $\gcd(P,Q) = 1$ or $\gcd(N,Q) = 1$. If N divides $U_{(N+1)/q}$ and $V_{(N+1)/2}$, then N divides $V_{(N+1)/2q}$.

Proof.

$$\frac{N+1}{2} = \frac{N+1}{2q} + \frac{N+1}{q}u \quad \text{with} \quad u = \frac{q-1}{2}.$$

By (IV.4):

$$2V_{(N+1)/2} = V_{(N+1)/2q}V_{[(N+1)/q]u} + DU_{(N+1)/2q}U_{[(N+1)/q]u}.$$

By (IV.15), N divides $U_{[(N+1)/q]u}$ so N divides $V_{(N+1)/2q}V_{[(N+1)/q]u}$.
   If $\gcd(P,Q) = 1$, by (IV.21) $\gcd(U_{[(N+1)/q]u}, V_{[(N+1)/q]u}) = 1$ or 2, hence $\gcd(N, V_{[(N+1)/q]u}) = 1$, so N divides $V_{(N+1)/2q}$.
   If $\gcd(N,Q) = 1$ and if there exists a prime p dividing N and $V_{[(N+1)/q]u}$, then by (IV.6) p also divides $4Q$; since p is odd, then $p \mid Q$, which is a contradiction. $\qquad\square$

Before indicating primality tests, it is easy to give sufficient conditions for a number to be composite:
   Let $N > 1$ be an odd integer. Assume that there exists a Lucas sequence $(U_n)_{n\geq 0}$ with parameters (P,Q), discriminant D, such that $\gcd(N, QD) = 1$, $(Q \mid N) = 1$, and $N \nmid U_{\frac{1}{2}[N-(D/N)]}$. Then N is composite.
   Similarly, assume that there exists a companion Lucas sequence $(V_n)_{n\geq 0}$, with parameters (P,Q), discriminant D, such that $N \nmid QD$, $(Q \mid N) = -1$ and $N \nmid V_{\frac{1}{2}[N-(D/N)]}$. Then N is composite.

Proof. Indeed, if $N = p$ is an odd prime not dividing QD, and if $(Q \mid p) = 1$, then $p \mid U_{\psi(p)/2}$, and similarly, if $(Q \mid p) = -1$, then $p \mid V_{\psi(p)/2}$, as stated in (IV.23). In both cases there is a contradiction. $\square$

Now I am ready to present several tests; each one better than the preceding one.

Test 1. Let $N > 1$ be an odd integer and $N + 1 = \prod_{i=1}^{s} q_i^{f_i}$. Assume that there exists an integer D such that $(D \mid N) = -1$, and for every prime factor q_i of $N + 1$, there exists a Lucas sequence $(U_n^{(i)})_{n \geq 0}$ with discriminant $D = P_i^2 - 4Q_i$, where $\gcd(P_i, Q_i) = 1$, or $\gcd(N, Q_i) = 1$ and such that $N \mid U_{N+1}^{(i)}$ and $N \nmid U_{(N+1)/q_i}^{(i)}$. Then N is a prime.

Defect of this test: it requires the knowledge of all the prime factors of $N + 1$ and the calculation of $U_n^{(i)}$ for $n = 1, 2, \ldots, N + 1$.

Proof. By (V.3), (V.4), $N \mid U_{\psi_D(N)}^{(i)}$ for every $i = 1, \ldots, s$. Let $\rho^{(i)}(N)$ be the smallest integer r such that $N \mid U_r^{(i)}$. By (IV.29) or (IV.22) and the hypothesis, $\rho^{(i)}(N) \mid (N + 1)$, $\rho^{(i)}(N) \nmid (N + 1)/q_i$, and also $\rho^{(i)}(N) \mid \psi_D(N)$. Hence $q_i^{f_i} \mid \rho^{(i)}(N)$ for every $i = 1, \ldots, s$. Therefore, $(N + 1) \mid \psi_D(N)$ and by (V.2), N is a prime. $\square$

The following test needs only half of the computations:

Test 2. Let $N > 1$ be an odd integer and $N + 1 = \prod_{i=1}^{s} q_i^{f_i}$. Assume that there exists an integer D such that $(D \mid N) = -1$, and for every prime factor q_i of $N + 1$, there exists a Lucas sequence $(V_n^{(i)})_{n \geq 0}$ with discriminant $D = P_i^2 - 4Q_i$, where $\gcd(P_i, Q_i) = 1$ or $\gcd(N, Q_i) = 1$, and such that $N \mid V_{(N+1)/2}^{(i)}$ and $N \nmid V_{(N+1)/2q_i}^{(i)}$. Then N is a prime.

Proof. By (IV.2), $N \mid U_{N+1}^{(i)}$. By (V.5), $N \nmid U_{(N+1)/q_i}^{(i)}$. By the test 1, N is a prime. $\square$

The following tests will require only a partial factorization of $N + 1$.

Test 3. Let $N > 1$ be an odd integer, let q be a prime factor of $N + 1$ such that $2q > \sqrt{N} + 1$. Assume that there exists a Lucas sequence $(V_n)_{n \geq 0}$, with discriminant $D = P^2 - 4Q$, where $\gcd(P, Q) = 1$ or

$\gcd(N, Q) = 1$, and such that $(D \mid N) = -1$, and $N \mid V_{(N+1)/2}$, $N \nmid V_{(N+1)/2q}$. Then N is a prime.

Defect of this test: it needs the knowledge of a fairly large prime factor of $N + 1$.

Proof. Let $N = \prod_{i=1}^{s} p_i^{e_i}$. By (IV.2), $N \mid U_{N+1}$, so by (IV.29) or (IV.22), $\rho(N) \mid (N + 1)$. By (V.5), $N \nmid U_{(N+1)/q}$; hence, $\rho(N) \nmid (N + 1)/q$, therefore $q \mid \rho(N)$. By (V.4) and (V.3), $N \mid U_{\psi_D(N)}$, so $\rho(N)$ divides $\psi_D(N)$, which in turn divides $N \prod_{i=1}^{s} (p_i - (D \mid p_i))$.

Since $q \nmid N$, then there exists p_i such that q divides $p_i - (D \mid p_i)$, thus $p_i \equiv (D \mid p_i) \pmod{2q}$. In conclusion, $p_i \geq 2q - 1 > \sqrt{N}$ and $1 \leq N/p_i < \sqrt{N} < 2q - 1$, and this implies that $N/p_i = 1$, that is, N is a prime. □

The next test, which was proposed by Morrison in 1975, may be viewed as the analogue of Pocklington's test indicated in Section III:

Test 4. Let $N > 1$ be an odd integer and $N + 1 = FR$, where $\gcd(F, R) = 1$ and the factorization of F is known. Assume that there exists D such that $(D \mid N) = -1$ and, for every prime q_i dividing F, there exists a Lucas sequence $(U_n^{(i)})_{n \geq 0}$ with discriminant $D = P_i^2 - 4Q_i$, where $\gcd(P_i, Q_i) = 1$ or $\gcd(N, Q_i) = 1$ and such that $N \mid U_{N+1}^{(i)}$ and $\gcd(U_{(N+1)/q_i}^{(i)}, N) = 1$. Then each prime factor p of N satisfies $p \equiv (D \mid p) \pmod{F}$. If, moreover, $F > \sqrt{N} + 1$, then N is a prime.

Proof. From the hypothesis, $\rho^{(i)}(N) \mid (N + 1)$; a fortiori, $\rho^{(i)}(p) \mid (N + 1)$. But $p \nmid U_{(N+1)/q}^{(i)}$, so $\rho^{(i)}(p) \mid (N + 1)/q_i$, by (IV.29) or (IV.22). If $q_i^{f_i}$ is the exact power of q_i dividing F, then $q_i^{f_i} \mid \rho^{(i)}(p)$, so by (IV.18), $q_i^{f_i}$ divides $p - (D \mid p)$, and this implies that F divides $p - (D \mid p)$.

Finally, if $F > \sqrt{N} + 1$, then $p + 1 \geq p - (D \mid p) \geq F > \sqrt{N} + 1$; hence, $p > \sqrt{N}$. This implies that N itself is a prime. □

The next result tells more about the possible prime factors of N.

(V.6)   Let N be an odd integer, $N + 1 = FR$, where $\gcd(F, R) = 1$ and the factorization of F is known. Assume that there exists a

Lucas sequence $(U_n)_{n \geq 0}$ with discriminant $D = P^2 - 4Q$, where $\gcd(P, Q) = 1$ or $\gcd(N, Q) = 1$ and such that $(D \mid N) = -1$, $N \mid U_{N+1}$, and $\gcd(U_F, N) = 1$. If p is a prime factor of N, then there exists a prime factor q of R such that $p \equiv (D \mid p) \pmod{q}$.

Proof. $\rho(p) \mid (p - (D \mid p))$ by (IV.18) and $\rho(p) \mid (N+1)$. But $p \nmid U_F$, so $\rho(p) \nmid F$. Hence, $\gcd(\rho(p), R) \neq 1$ and there exists a prime q such that $q \mid R$ and $q \mid \rho(p)$; in particular, $p \equiv (D \mid p) \pmod{q}$.   □

This result is used in the following test:

Test 5. Let $N > 1$ be an odd integer and $N + 1 = FR$, where $\gcd(F, R) = 1$, the factorization of F is known, R has no prime factor less than B, where $BF > \sqrt{N} + 1$. Assume that there exists D such that $(D \mid N) = -1$ and the following conditions are satisfied:

(i) For every prime q_i dividing F, there exists a Lucas sequence $(U_n^{(i)})_{n \geq 0}$, with discriminant $D = P_i^2 - 4Q_i$, where $\gcd(P_i, Q_i) = 1$ or $\gcd(N, Q_i) = 1$ and such that $N \mid U_{N+1}^{(i)}$ and $\gcd(U_{(N+1)/q_i}^{(i)}, N) = 1$.

(ii) There exists a Lucas sequence $(U_n')_{n \geq 0}$, with discriminant $D = P'^2 - 4Q'$, where $\gcd(P', Q') = 1$ or $\gcd(N, Q') = 1$ and such that $N \mid U_{N+1}'$ and $\gcd(U_F', N) = 1$.

Then N is a prime.

Proof. Let p be a prime factor of N. By Test 4, $p \equiv (D \mid p) \pmod{F}$ and by the preceding result, there exists a prime factor q of R such that $p \equiv (D \mid p) \pmod{q}$. Hence, $p \equiv (D \mid p) \pmod{qF}$ and so,

$$p + 1 \geq p - (D \mid p) \geq qF \geq BF > \sqrt{N} + 1.$$

Therefore, $p > \sqrt{N}$ and N is a prime number.   □

The preceding test is more flexible than the others, since it requires only a partial factorization of $N + 1$ up to a point where it may be assured that the nonfactored part of $N+1$ has no factors less than B.

Now I want to indicate, in a very succinct way, how to quickly calculate the terms of Lucas sequences with large indices. One of the methods is similar to that used in the calculations of high powers, which was indicated in Section III.

Write $n = n_0 2^k + n_1 2^{k-1} + \cdots + n_k$, with $n_i = 0$ or 1 and $n_0 = 1$; so $k = [(\log n)/(\log 2)]$. To calculate U_n (or V_n) it is necessary to perform the simultaneous calculation of U_m, V_m for various values of m. The following formulas are needed:

$$\begin{cases} U_{2j} = U_j V_j, \\ V_{2j} = V_j^2 - 2Q^j, \end{cases} \qquad \text{[see formulas (IV.2)]}$$

$$\begin{cases} 2U_{2j+1} = V_{2j} + PU_{2j}, \\ 2V_{2j+1} = PV_{2j} + DU_{2j}. \end{cases} \qquad \text{[see formulas (IV.5)]}$$

Put $s_0 = n_0 = 1$, and $s_{j+1} = 2s_j + n_{j+1}$. Then $s_k = n$. So, it suffices to calculate U_{s_j}, V_{s_j} for $j \leq k$; note that

$$U_{s_{j+1}} = U_{2s_j + n_{j+1}} = \begin{cases} U_{2s_j} & \text{or} \\ U_{2s_j+1}, \end{cases}$$

$$V_{s_{j+1}} = V_{2s_j + n_{j+1}} = \begin{cases} V_{2s_j} & \text{or} \\ V_{2s_j+1}. \end{cases}$$

Thus, it is sufficient to compute $2k$ numbers U_i and $2k$ numbers V_i, that is, only $4k$ numbers.

If it is needed to know U_n modulo N, then in all steps the numbers may be replaced by their least positive residues modulo N.

The second method is also very quick. For $j \geq 1$,

$$\begin{pmatrix} U_{j+1} & V_{j+1} \\ U_j & V_j \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_j & V_j \\ U_{j-1} & V_{j-1} \end{pmatrix}.$$

If

$$M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix},$$

then

$$\begin{pmatrix} U_n & V_n \\ U_{n-1} & V_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} U_1 & V_1 \\ 0 & 2 \end{pmatrix}.$$

To find the powers of M, say M^m, write m in binary form and proceed in the manner followed to calculate a power of a number.

If U_n modulo N is to be determined, all the numbers appearing in the above calculation should be replaced by their least positive residues modulo N.

To conclude this section, I would like to stress that there are many other primality tests of the same family, which are appropriate for numbers of certain forms, and use either Lucas sequences or other similar sequences.

Sometimes it is practical to combine tests involving Lucas sequences with the tests discussed in Section III; see the paper of Brillhart, Lehmer & Selfridge (1975). As a comment, I add (half-jokingly) the following rule of thumb: the longer the statement of the testing procedure, the quicker it leads to a decision about the primality.

The tests indicated so far are applicable to numbers of the form $2^n - 1$ (see Section VII on Mersenne numbers, where the test will be given explicitly), but also to numbers of the form $k \times 2^n - 1$ (see, for example, Inkeri's paper of 1960 or Riesel's book, 1985).

In 1998, H.C. Williams published a book dedicated to a historical and mathematical study of the work of Lucas. His authoritative and thorough treatment is recommended to anyone who wants to learn more than I could include in my succinct presentation.

VI Fermat Numbers

For numbers having a special form, there are more suitable methods to test whether they are prime or composite.

The numbers of the form $2^m + 1$ were considered long ago.

If $2^m + 1$ is a prime, then m must be of the form $m = 2^n$, so it is a Fermat number, $F_n = 2^{2^n} + 1$.

The Fermat numbers $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are primes. Fermat believed, and tried to prove, that all Fermat numbers are primes. Since F_5 has 10 digits, in order to test its primality, it would be necessary to have a table of primes up to $100\,000$ (which was unavailable to him) or to derive and use some criterion for a number to be a factor of a Fermat number. This, Fermat failed to do.

Euler showed that every factor of F_n (with $n \geq 2$) must be of the form $k \times 2^{n+2} + 1$ and thus he discovered that 641 divides F_5:

$$F_5 = 641 \times 6700417.$$

Proof. It suffices to show that every prime factor p of F_n is of the form indicated. Since $2^{2^n} \equiv -1 \pmod{p}$, then $2^{2^{n+1}} \equiv 1 \pmod{p}$,

so 2^{n+1} is the order of 2 modulo p. By Fermat's little theorem 2^{n+1} divides $p-1$; in particular, 8 divides $p-1$. Therefore the Legendre symbol is $2^{(p-1)/2} \equiv (2 \mid p) \equiv 1 \pmod{p}$, and so 2^{n+1} divides $(p-1)/2$; this shows that $p = k \times 2^{n+2} + 1$. $\qquad\qquad\square$

Since the numbers F_n increase very rapidly with n, it becomes laborious to check their primality.

Using the converse of Fermat's little theorem, as given by Lucas, Pepin obtained in 1877 a test for the primality of Fermat numbers. Namely:

Pepin's Test. Let $F_n = 2^{2^n} + 1$ (with $n \geq 2$) and $k \geq 2$. Then, the following conditions are equivalent:

(i) F_n is prime and $(k \mid F_n) = -1$.

(ii) $k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

Proof. If (i) is assumed, then by Euler's criterion for the Legendre symbol

$$k^{(F_n-1)/2} \equiv \left(\frac{k}{F_n}\right) \equiv -1 \pmod{F_n}.$$

If, conversely, (ii) is supposed true, let a, $1 \leq a < F_n$, be such that $a \equiv k \pmod{F_n}$. Since $a^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, then $a^{F_n-1} \equiv 1 \pmod{F_n}$. By Test 3 in Section III, F_n is prime. Hence

$$\left(\frac{k}{F_n}\right) \equiv k^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \qquad\qquad\square$$

Possible choices of k are $k = 3, 5, 10$, because $F_n \equiv 2 \pmod 3$, $F_n \equiv 2 \pmod 5$, $F_n \equiv 1 \pmod 8$; hence, by Jacobi's reciprocity law

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

$$\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

$$\left(\frac{10}{F_n}\right) = \left(\frac{2}{F_n}\right)\left(\frac{5}{F_n}\right) = -1.$$

This test is very practical in application. However, if F_n is composite, the test does not indicate any factor of F_n.

Lucas used it to show that F_6 is composite, and in 1880, at the age of 82, Landry showed that

$$F_6 = 274177 \times 67280421310721.$$

Landry never described how he factored F_6. In a historical reconstitution, Williams (1993) gives indications, obtained from clues in Landry's letters and work, of the method used by Landry.

But the best of the story is a recent "coup de théâtre". In a biography of Clausen by Biermann (1964), it is stated that in a letter to Gauss of January 1, 1855, Clausen (who was known as an able calculator and an important astronomer) already gave the complete factorization of F_6. In this letter, which remains in the library of the University of Göttingen, Clausen also expressed his belief that the larger of the two factors was the largest prime number known at that time. Curiously, the corresponding remark in Biermann's biography remained widely unnoticed for many years.

Generally, the factorization of Fermat numbers known to be composite has been the object of intensive research. In the following table we give the current state of this matter. The notation Pn indicates a prime number of n digits, while Cn denotes a composite number having n digits.

<div align="center">

Table 6.   Completely factored Fermat numbers

</div>

$F_5 = 641 \times 6700417$

$F_6 = 274177 \times 67280421310721$

$F_7 = 59649589127497217 \times 5704689200685129054721$

$F_8 = 1238926361552897 \times P62$

$F_9 = 2424833 \times$
       $7455602825647884208337395736200454918783366342657 \times P99$

$F_{10} = 45592577 \times 6487031809 \times$
       $4659775785220018543264560743076778192897 \times P252$

$F_{11} = 319489 \times 974849 \times 167988556341760475137 \times$
       $3560841906445833920513 \times P564$

Notes.

F_5 : Euler (1732)

F_6 : factor 1 Clausen (unpublished, 1855), Landry and Le Lasseur (1880)

F_7 : Morrison and Brillhart (1970)

F_8 : factor 1 Brent and Pollard (1980)

F_9 : factor 1 Western (1903),
    other factors A.K. Lenstra and Manasse (1990)

F_{10} : factor 1 Selfridge (1953), factor 2 Brillhart (1962),
    other factors Brent (1995)

F_{11} : factors 1 and 2 Cunningham (1899), other factors Brent (1988),
    primality of factor 5 Morain (1988)

It is quite difficult to keep track of all the new results that accumulate rapidly, but also to remain acquainted with the most recent methods developed for the factorization of such numbers. In this regard, the articles of Brent (1999), and of Brent, Crandall, Dilcher & van Halewyn (2000) are very informative. I thank W. Keller for keeping me up-to-date on developments concerning the Fermat numbers.

Table 7.   Incomplete factorizations of Fermat numbers

$$F_{12} = 114689 \times 26017793 \times 63766529 \times 190274191361 \times$$
$$1256132134125569 \times C1187$$
$$F_{13} = 2710954639361 \times 2663848877152141313 \times$$
$$3603109844542291969 \times 319546020820551643220672513 \times C2391$$
$$F_{15} = 1214251009 \times 2327042503868417 \times$$
$$168768817029516972383024127016961 \times C9808$$
$$F_{16} = 825753601 \times 188981757975021318420037633 \times C19694$$
$$F_{17} = 31065037602817 \times C39444$$
$$F_{18} = 13631489 \times 81274690703860512587777 \times C78884$$
$$F_{19} = 70525124609 \times 646730219521 \times C157804$$
$$F_{21} = 4485296422913 \times C631294$$
$$F_{23} = 167772161 \times C2525215$$

Table 8.   Composite Fermat numbers without known factor

F_{14} :	Selfridge and Hurwitz (1963)
F_{20} :	Buell and Young (1987)
F_{22} :	Crandall, Doenias, Norrie and Young (1993),
	independently by Carvalho and Trevisan (1993)
F_{24} :	Mayer, Papadopoulos and Crandall (1999)

The smallest Fermat numbers of unknown character are: F_{33}, F_{34}, F_{35}, F_{40}, F_{41}, F_{44}, ...

RECORDS

A.   The largest known Fermat prime is $F_4 = 65537$.

B.   The largest known composite Fermat number is $F_{2145351}$, which has the factor $3 \times 2^{2145353} + 1$. This 645817-digit factor was discovered by J.B. Cosgrave and his Proth-Gallot Group at St. Patrick's College (Dublin, Ireland) on February 21, 2003. Programs of P. Jobling, G. Woltman and Y. Gallot were essential for the discovery.

C.   As of the end of May 2003, there was a total of 214 Fermat numbers known to be composite.

Here are some open problems:

(1) Are there infinitely many prime Fermat numbers?

This question became significant with the famous result of Gauss (see *Disquisitiones Arithmeticae*, articles 365, 366—the last ones in the book—as a crowning result for much of the theory previously developed). He showed that if $n \geq 3$ is an integer, and if the regular polygon with n sides may be constructed by ruler and compass, then $n = 2^k p_1 p_2 \cdots p_h$, where $k \geq 0$, $h \geq 0$ and $p_1, \ldots, p_h$ are distinct odd primes, each being a Fermat number.

In 1844, Eisenstein proposed, as a problem, to prove that there are indeed infinitely many prime Fermat numbers. I should add, that already in 1828, an anonymous writer stated that

$$2 + 1, \ 2^2 + 1, \ 2^{2^2} + 1, \ 2^{2^{2^2}} + 1, \ 2^{2^{2^{2^2}}} + 1, \ \ldots$$

are all primes, and added that they are the only prime Fermat numbers (apart from $2^{2^3} + 1$). However, Selfridge discovered in 1953 a factor of F_{16}, which therefore is not a prime, and this fact disproved that conjecture.

(2) Are there infinitely many composite Fermat numbers?

Questions (1) and (2) seem beyond the reach of present-day methods and, side by side, they show how little is known on this matter.

(3) Is every Fermat number square-free (i.e., without square factors)?

It has been conjectured, for example by Lehmer and by Schinzel, that there exist infinitely many square-free Fermat numbers.

It is not difficult to show that if p is a prime number and p^2 divides some Fermat number, then $2^{p-1} \equiv 1 \pmod{p^2}$—this will be proved in detail in Chapter 5, Section III. Since Fermat numbers are pairwise relatively prime, if there exist infinitely many Fermat numbers with a square factor, then there exist infinitely many primes p satisfying the above congruence.

I shall discuss this congruence in Chapter 5. Let it be said here that it is very rarely satisfied. In particular, it is not known whether it holds infinitely often.

Sierpiński considered in 1958 the numbers of the form $S_n = n^n + 1$, with $n \geq 2$. He proved that if S_n is a prime, then there exists $m \geq 0$ such that $n = 2^{2^m}$, so S_n is a Fermat number:

$$S_n = F_{m+2^m}.$$

It follows that the only numbers S_n which are primes and have less than 3×10^{20} digits, are 5 and 257. Indeed, if $m = 0, 1$ one has $F_1 = 5$, $F_3 = 257$; if $m = 2, 3, 4$ or 5, we have F_6, F_{11}, F_{20} and F_{37}, which are composite numbers. For $m = 5$, one obtains F_{70}, which is not known to be prime or composite. Since $2^{10} > 10^3$, then

$$F_{70} > 2^{2^{70}} > 2^{10^{21}} = (2^{10})^{10^{20}} > 10^{3 \times 10^{20}}.$$

The primes of the form $n^n + 1$ are very rare. Are there only finitely many such primes? If so, there are infinitely many composite Fermat numbers. But all this is pure speculation, with no basis for any reasonable conjecture.

The recent book by 3 authors (Křížek, Luca & Somer), entitled *17 Lectures on Fermat's Last* (oops) *Numbers*, contains 257 pages of very interesting facts around the Fermat numbers. With the rapid progress in the study of these numbers, I ask to my readers: How many pages will have the next book on Fermat numbers?

VII   Mersenne Numbers

If a number of the form $2^m - 1$ is a prime, then $m = q$ is a prime. Even more, it is not a difficult exercise to show that if $2^m - 1$ is a

prime power, it must be a prime, and so m is a prime. [If you cannot do it alone, look at the paper of Ligh & Neal (1974).]

The numbers $M_q = 2^q - 1$ (with q prime) are called Mersenne numbers, and their consideration was motivated by the study of perfect numbers (see the addendum to this section).

Already at Mersenne's time, it was known that some Mersenne numbers were prime, others composite. For example, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$ are primes, while $M_{11} = 23 \times 89$. In 1640, Mersenne stated that M_q is also a prime for $q = 13$, 17, 19, 31, 67, 127, 257; he was wrong about 67 and 257, and he did not include 61, 89, 107 (among those less than 257), which also produce Mersenne primes. Yet, his statement was quite astonishing, in view of the size of the numbers involved.

The obvious problem is to recognize if a Mersenne number is a prime, and if not, to determine its factors.

A classical result about factors was stated by Euler in 1750 and proved by Lagrange (1775) and again by Lucas (1878):

If q is a prime $q \equiv 3 \pmod 4$, then $2q + 1$ divides M_q if and only if $2q + 1$ is a prime; in this case, if $q > 3$, then M_q is composite.

Proof. Let $n = 2q + 1$ be a factor of M_q. Since $2^2 \not\equiv 1 \pmod n$, $2^q \not\equiv 1 \pmod n$, $2^{2q} - 1 = (2^q + 1)M_q \equiv 0 \pmod n$, then by Lucas test 3 (see Section III), n is a prime.

Conversely, let $p = 2q + 1$ be a prime. Since $p \equiv 7 \pmod 8$, then $(2 \mid p) = 1$, so there exists m such that $2 \equiv m^2 \pmod p$. It follows that $2^q \equiv 2^{(p-1)/2} \equiv m^{p-1} \equiv 1 \pmod p$, so p divides M_q.

If, moreover, $q > 3$, then $M_q = 2^q - 1 > 2q + 1 = p$, so M_q is composite.   □

Thus if $q = 11$, 23, 83, 131, 179, 191, 239, 251, then M_q has the factor 23, 47, 167, 263, 359, 383, 479, 503, respectively.

Around 1825, Sophie Germain considered, in connection with Fermat's last theorem, the primes q such that $2q + 1$ is also a prime. These primes are now called *Sophie Germain primes*, and I shall return to them in Chapter 5.

It is also very easy to determine the form of the factors of Mersenne numbers:

If n divides M_q ($q > 2$), then $n \equiv \pm 1 \pmod 8$ and $n \equiv 1 \pmod q$.

Proof. It suffices to show that each prime factor p of M_q is of the form indicated.

If p divides $M_q = 2^q - 1$, then $2^q \equiv 1 \pmod{q}$; so by Fermat's little theorem, q divides $p - 1$, that is, $p - 1 = 2kq$ (since $p \neq 2$). So

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv 2^{qk} \equiv 1 \pmod{p},$$

therefore $p \equiv \pm 1 \pmod{8}$, by the property of the Legendre symbol already indicated in Section II.   □

The primality of M_{13} and M_{17} was determined by Cataldi using trial division. Euler also used trial division to show that M_{31} is a prime, but he could spare many calculations, in view of the above mentioned form of factors of Mersenne numbers. In this respect, see Williams & Shallit (1994).

The best method presently known to find out whether M_q is a prime or a composite number is based on the computation of a recurring sequence, indicated by Lucas (1878), and Lehmer (1930, 1935); see also Western (1932), Hardy & Wright (1938, p. 223), and Kaplansky (1945). However, explicit factors cannot be found in this manner.

If n is odd, $n \geq 3$, then $M_n = 2^n - 1 \equiv 7 \pmod{12}$. Also, if $N \equiv 7 \pmod{12}$, then the Jacobi symbol

$$\left(\frac{3}{N}\right) = \left(\frac{N}{3}\right)(-1)^{(N-1)/2} = -1.$$

Primality test for Mersenne numbers. Let $P = 2$, $Q = -2$, and consider the associated Lucas sequences $(U_m)_{m \geq 0}$, $(V_m)_{m \geq 0}$, which have discriminant $D = 12$. Then $N = M_n$ is a prime if and only if N divides $V_{(N+1)/2}$.

Proof. Let N be a prime. By (IV.2)

$$V_{(N+1)/2}^2 = V_{N+1} + 2Q^{(N+1)/2} = V_{N+1} - 4(-2)^{(N-1)/2}$$

$$\equiv V_{N+1} - 4\left(\frac{-2}{N}\right) \equiv V_{N+1} + 4 \pmod{N},$$

because

$$\left(\frac{-2}{N}\right) = \left(\frac{-1}{N}\right)\left(\frac{2}{N}\right) = -1,$$

since $N \equiv 3 \pmod 4$ and $N \equiv 7 \pmod 8$. Thus it suffices to show that $V_{N+1} \equiv -4 \pmod N$.

By (IV.4), $2V_{N+1} = V_N V_1 + DU_N U_1 = 2V_N + 12U_N$; hence, by (IV.14) and (IV.13):

$$V_{N+1} = V_N + 6U_N \equiv 2 + 6(12 \mid N) \equiv 2 - 6 \equiv -4 \pmod N.$$

Conversely, assume that N divides $V_{(N+1)/2}$. Then N divides U_{N+1} [by (IV.2)]. Also, by (IV.6) $V_{(N+1)/2}^2 - 12U_{(N+1)/2}^2 = 4(-1)^{(N+1)/2}$; hence $\gcd(N, U_{(N+1)/2}) = 1$. Since $\gcd(N, 2) = 1$, then by the Test 1 (Section V), N is a prime.   □

For the purpose of calculation, it is convenient to replace the Lucas sequence $(V_m)_{m \geq 0}$ by the following sequence $(S_k)_{k \geq 0}$, defined recursively as follows:

$$S_0 = 4, \qquad S_{k+1} = S_k^2 - 2;$$

thus, the sequence begins with 4, 14, 194, ... Then the test is phrased as follows:

$M_n = 2^n - 1$ *is prime if and only if* M_n *divides* S_{n-2}.

Proof. $S_0 = 4 = V_2/2$. Assume that $S_{k-1} = V_{2^k}/2^{2^{k-1}}$; then

$$S_k = S_{k-1}^2 - 2 = \frac{V_{2^k}^2}{2^{2^k}} - 2 = \frac{V_{2^{k+1}} + 2^{2^{k+1}}}{2^{2^k}} - 2 = \frac{V_{2^{k+1}}}{2^{2^k}}.$$

By the test, M_n is prime if and only if M_n divides

$$V_{(M_n+1)/2} = V_{2^{n-1}} = 2^{2^{n-2}} S_{n-2},$$

or equivalently, M_n divides S_{n-2}.   □

The repetitive nature of the computations makes this test quite suitable. In this way, all examples of large Mersenne primes have been discovered. Lucas himself showed, in 1876, that M_{127} is a prime, while M_{67} is composite. Not much later, Pervushin showed that M_{61} is also a prime. Finally, in 1927 (published in 1932) Lehmer showed that M_{257} is also composite, settling one way or another, what Mersenne had asserted. Note that M_{127} has 39 digits and was the largest prime

known before the age of computers. In this competition this was the longest lasting record!

The Mersenne primes with $q \leq 127$ were discovered before the computer age. A. Turing made, in 1951, the first attempt to find Mersenne primes using an electronic computer; however, he was unsuccessful. In 1952, Robinson carried out Lucas' test using a computer SWAC (from the National Bureau of Standards in Los Angeles), with the assistance of D.H. and E. Lehmer. He discovered the Mersenne primes M_{521}, M_{607} on January 30, 1952—the first such discoveries with a computer. The primes M_{1279}, M_{2203}, M_{2281} were found later in the same year.

The Lucas-Lehmer primality test for Mersenne numbers M_q, when q is large, requires much calculation. To face this situation, the work has to be done by teams, using very powerful computers. Moreover, one uses programs especially created for the purpose. A great role is played by multiplication done via the fast Fourier transform, invented by Schönhage & Strassen in 1971. The programs of Crandall and Woltman have been determinant in the discovery of large primes.

The GIMPS ("Great Internet Mersenne Prime Search"), organized by Woltman, has as its aim to discover large Mersenne primes. Anyone, so willing, may participate with his personal computer. He will receive the software and an interval of prime exponents as his territory for search. Presently the project has recruited several thousands participants.

In a not so distant past the gold and diamond prospectors sacrificed family and friends going to inhospitable places, jungles with snakes, disease infested marshes, or high mountains with cliffs and snow, all this in search of the precious discovery which would make them rich. The modern searcher of Mersenne primes lives a transposed but similar adventure. The location of his findings cannot be anticipated; lucky the one who first finds IT. No riches, but fame. My metaphor is not so different from reality. I suggest you learn the ways to the 38th Mersenne prime in Woltman's own description (1999)—the captain explorer tells . . .

RECORD

The first 38 Mersenne primes are shown in Table 9. The largest known Mersenne prime, with $q = 13466917$, has 4053946 digits. Its discovery, which occurred on November 14, 2001, is credited to

M. Cameron, G.F. Woltman, S. Kurowski, and to GIMPS. The fact is that Cameron found that prime working on a segment assigned to him by GIMPS.

Note that this Mersenne prime is currently the largest known prime, and only the second *megaprime* known, i.e., a prime with one million digits at least.

It should be remarked that the prime M_{110503} was found only after M_{132049} and M_{216091} were known. So it may happen that the next Mersenne prime to be found has $q < 13466917$, since not all of the primes q below this limit have been tested to see if M_q is a prime.

On the other hand, the search for Sophie Germain primes q of the form $q = k \times 2^N - 1$ (so, $2q + 1$ is also a prime) yields, as already indicated, composite Mersenne numbers M_q.

RECORD

The largest Mersenne number M_q known to be composite has $q = 2540041185 \times 2^{114729} - 1$ and was found by D. Underbakke, G.F. Woltman and Y. Gallot in January 2003. The prime q is the largest known Sophie Germain prime (see Chapter 5, Section II).

Riesel's book (1985) has a table of complete factorization of all numbers $M_n = 2^n - 1$, with n odd, $n \leq 257$. A more extensive table is in the book of Brillhart et al. (1983, 1988; see also the third edition, 2002).

Just as for Fermat numbers, there are many open problems about Mersenne numbers:

(1) Are there infinitely many Mersenne primes?

(2) Are there infinitely many composite Mersenne numbers?

The answer to both questions ought to be "yes", as I will try to justify. For example, I will indicate in Chapter 6, Section A, after (D5), that some sequences, similar to the sequence of Mersenne numbers, contain infinitely many composite numbers.

(3) Is every Mersenne number square-free?

Table 9. Mersenne primes M_q with $q < 7000000$

q	Year	Discoverer
2	–	–
3	–	–
5	–	–
7	–	–
13	1461	Anonymous*
17	1588	P.A. Cataldi
19	1588	P.A. Cataldi
31	1750	L. Euler
61	1883	I.M. Pervushin
89	1911	R.E. Powers
107	1913	E. Fauquembergue
127	1876	E. Lucas
521	1952	R.M. Robinson
607	1952	R.M. Robinson
1279	1952	R.M. Robinson
2203	1952	R.M. Robinson
2281	1952	R.M. Robinson
3217	1957	H. Riesel
4253	1961	A. Hurwitz
4423	1961	A. Hurwitz
9689	1963	D.B. Gillies
9941	1963	D.B. Gillies
11213	1963	D.B. Gillies
19937	1971	B. Tuckerman
21701	1978	L.C. Noll and L. Nickel
23209	1979	L.C. Noll
44497	1979	H. Nelson and D. Slowinski
86243	1982	D. Slowinski
110503	1988	W.N. Colquitt and L. Welsh, Jr.
132049	1983	D. Slowinski
216091	1985	D. Slowinski
756839	1992	D. Slowinski and P. Gage
859433	1993	D. Slowinski and P. Gage
1257787	1996	D. Slowinski and P. Gage
1398269	1996	J. Armengaud, G.F. Woltman and GIMPS
2976221	1997	G. Spence, G.F. Woltman and GIMPS
3021377	1998	R. Clarkson, G.F. Woltman, S. Kurowski and GIMPS
6972593	1999	N. Hajratwala, G.F. Woltman, S. Kurowski and GIMPS

*See Dickson's *History of the Theory of Numbers*, Vol. I, p. 6.

Rotkiewicz showed in 1965 that if p is a prime and p^2 divides some Mersenne number, then $2^{p-1} \equiv 1 \pmod{p^2}$, the same congruence which already appeared in connection with Fermat numbers having a square factor.

I wish to mention two other problems involving Mersenne numbers, one of which has been solved, while the other one is still open.

Is it true that if M_q is a Mersenne prime, then M_{M_q} is also a prime number?

The answer is negative, since despite M_{13} being prime, $M_{M_{13}} = 2^{8191} - 1$ is composite; this was shown by Wheeler, see Robinson (1954). Note that $M_{M_{13}}$ has more than 2400 digits. In 1976, Keller discovered the prime factor

$$p = 2 \times 20644229 \times M_{13} + 1 = 338193759479$$

of the Mersenne number $M_{M_{13}}$, thus providing an easier proof that it is composite; only 13 squarings modulo p are needed to verify that $2^{2^{13}} \equiv 2 \pmod{p}$. This has been communicated to me by Keller in a letter.

The second problem, proposed by Catalan in 1876 and reported in Dickson's *History of the Theory Numbers*, Vol. I, p. 22, is the following. Consider the sequence of numbers

$$
\begin{aligned}
C_1 &= 2^2 - 1 = 3 = M_2\,, \\
C_2 &= 2^{C_1} - 1 = 7 = M_3\,, \\
C_3 &= 2^{C_2} - 1 = 127 = M_7\,, \\
C_4 &= 2^{C_3} - 1 = 2^{127} - 1 = M_{127}\,, \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
C_{n+1} &= 2^{C_n} - 1 \\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}
$$

Are all numbers C_n primes? Are there infinitely many which are prime? At present, it is impossible to test C_5, which has more than 10^{37} digits!

I conclude with the interesting conjecture of Bateman, Selfridge & Wagstaff (1989), concerning the Mersenne primes.

Conjecture. Let p be an odd natural number (not necessarily a prime). If two of the following conditions are satisfied, so is the third one:

(a) p is equal to $2^k \pm 1$ or to $4^k \pm 3$ (for some $k \geq 1$).

(b) M_p is a prime.

(c) $(2^p + 1)/3$ is a prime.

In a private communication, H. and R. Lifchitz informed that the conjecture holds for all $p < 720000$. In this range, the only primes satisfying the three conditions are $p = 3, 5, 7, 13, 17, 19, 31, 61, 127$. It is conceivable that these are the only primes for which the above three conditions hold.

ADDENDUM ON PERFECT NUMBERS

I shall now consider perfect numbers and tell how they are related to Mersenne numbers.

A natural number $n > 1$ is said to be *perfect* if it is equal to the sum of all its aliquot parts, that is, its divisors d, with $d < n$. For example, $n = 6, 28, 496, 8128$ are the perfect numbers smaller than 10000.

Perfect numbers were already known in ancient times. The first perfect number 6 was connected, by mystic and religious writers, to perfection, thus explaining that the Creation required 6 days, so PERFECT is the world.

Euclid showed, in his *Elements*, Book IX, Proposition 36, that if q is a prime and $M_q = 2^q - 1$ is a prime, then $N = 2^{q-1}(2^q - 1)$ is a perfect number.

In a posthumous paper, Euler proved the converse: any even perfect number is of the form indicated by Euclid. Thus, the knowledge of even perfect numbers is equivalent to the knowledge of Mersenne primes.

And what about odd perfect numbers? Do they exist? Not even one has ever been found! This is a question which has been extensively searched, but its answer is still unknown.

Quick information on the progress made toward the solution of the problem may be found in Guy's book (new edition 1994), quoted in General References. More recent facts are also mentioned below.

The methods to tackle the problem have been legion. I believe it is useful to describe them so the reader will get a feeling of what to do when nothing seems reasonable. The idea is to assume that there exists an odd perfect number N and to derive various consequences, concerning the number $\omega(N)$ of its distinct prime factors, the size of N, the multiplicative form, and the additive form of N, etc. I shall review what has been proved in each count.

(a) Number of distinct prime factors $\omega(N)$

Hagis (1980, announced in 1975) proved that $\omega(N) \geq 8$. The same result was also obtained by Chein (1979) in his thesis.

In 1983, Hagis and, independently, Kishore proved that if $3 \nmid N$, then $\omega(N) \geq 11$.

Another result in this line was given by Dickson in 1913: for every $k \geq 1$ there are at most finitely many odd perfect numbers N, such that $\omega(N) = k$. In 1949, Shapiro gave a simpler proof.

Dickson's theorem was generalized in 1956 by Kanold, for numbers N satisfying the condition $\sigma(N)/N = \alpha$ (α is a given rational number and $\sigma(N)$ denotes the sum of all divisors of N). The proof involved the fact that the equation $aX^3 - bY^3 = c$ has at most finitely many solutions in integers x, y. Since an effective estimate for the number of solutions was given by Baker, with his celebrated method of linear forms in logarithms, it became possible for Pomerance to show in 1977 (taking $\alpha = 2$), for every $k \geq 1$: If the odd perfect number N has k distinct prime factors, then

$$N < (4k)^{(4k)^{2^{k^2}}}.$$

In 1994, Heath-Brown sharpened substantially the result of Pomerance: If an odd perfect number N has k distinct prime factors, then

$$N < 4^{4^k}.$$

Improving further, Cook (1999) showed that the base 4 may be replaced by $195^{1/7} = 2.123\ldots$.

(b) Lower bound for N

Brent, Cohen & te Riele (1991) have established that if N is an odd perfect number, then $N > 10^{300}$. Previously, in 1989, Brent & Cohen showed that $N > 10^{160}$, and in 1973 Hagis proved that $N > 10^{50}$.

In 1976, Buxton & Elmore claimed that $N > 10^{200}$, but this statement has not been substantiated in detail, so it should not be accepted. In 1999, Grytczuk & Wojtowicz published a far larger lower bound for N, but F. Saidak found a flaw in the proof, and this was acknowledged by the authors in 2000.

(c) Multiplicative structure of N

The first result is by Euler: $N = p^e k^2$, where p is a prime not dividing k, and $p \equiv e \equiv 1 \pmod 4$.

There have been numerous results on the kind of number k. For example, in 1972 Hagis & McDaniel showed that k is not a cube.

(d) Largest prime factor of N

In 1998, Hagis & Cohen showed that N must have a prime factor greater than 10^6. Earlier, in 1975, Hagis & McDaniel had proved that the largest prime factor of N should be greater than 100110.

For prime-power factors, Muskat showed in 1966 that N must have one which is greater than 10^{12}.

(e) Other prime factors of N

In 1975, Pomerance showed that the second largest prime factor of N should be at least 139. That limit was raised to 10^3 by Hagis (1981) and to 10^4 by Iannucci (1999). In 2000, Iannucci also showed that the third largest prime factor of N exceeds 100.

In 1952, Grün showed that the smallest prime factor p_1 of N should satisfy the relation $p_1 < \frac{2}{3}\omega(N) + 2$.

In his thesis, Kishore (1977) showed that if $i = 2, 3, 4, 5, 6$, the ith smallest prime factor of N is less than $2^{2^{i-1}}(\omega(N) - i + 1)$.

In 1958, Perisastri proved that

$$\frac{1}{2} < \sum_{p|N} \frac{1}{p} < 2\log\frac{\pi}{2}.$$

This has been sharpened by Suryanarayana (1963), Suryanarayana & Hagis (1970), and Cohen (1978).

(f) Additive structure of N

In 1953, Touchard proved that $N \equiv 1 \pmod{12}$ or $N \equiv 9 \pmod{36}$. An easier proof was later given by Satyanarayana (1959).

(g) Ore's conjecture

In 1948, Ore considered the harmonic mean of the divisors of N, namely,

$$H(N) = \frac{\tau(N)}{\sum_{d|N}(1/d)},$$

where $\tau(N)$ denotes the number of divisors of N.

If N is a perfect number, then $H(N)$ is an integer; indeed, whether N is even or odd, this follows from Euler's results.

Actually, Laborde noted in 1955, that N is an even perfect number if and only if

$$N = 2^{H(N)-1}\big(2^{H(N)} - 1\big),$$

hence $H(N)$ is an integer, and in fact a prime.

Ore conjectured that if N is odd, then $H(N)$ is not an integer. The truth of this conjecture would imply, therefore, that there do not exist odd perfect numbers.

Ore verified that the conjecture is true if N is a prime-power or if $N < 10^4$. Since 1954 (published only in 1972), Mills checked its truth for $N < 10^7$, as well as for numbers of special form, in particular, if all prime-power factors of N are smaller than 65551^2.

Pomerance (unpublished) verified Ore's conjecture when $\omega(N) \leq 2$, by showing that if $\omega(N) \leq 2$ and $H(N)$ is an integer, then N is an even perfect number (kindly communicated to me by letter).

The next results do not distinguish between even or odd perfect numbers. They concern the distribution of perfect numbers. The idea is to define, for every $x \geq 1$, the function $V(x)$, which counts the perfect numbers less or equal to x:

$$V(x) = \#\{N \text{ perfect} \mid N \leq x\}.$$

The limit $\lim_{x \to \infty} V(x)/x$ represents a natural density for the set of perfect numbers. In 1954, Kanold showed the $\lim_{x \to \infty} V(x)/x = 0$. Thus, $V(x)$ grows to infinity slower than x does.

The following more precise result of Wirsing (1959) tells how slowly $V(x)$ grows: there exist x_0 and $C > 0$ such that if $x \geq x_0$ then

$$V(x) \leq e^{(C \log x)/(\log\log x)}.$$

Earlier work was done by Hornfeck (1955, 1956), Kanold (1957), and Hornfeck & Wirsing (1957), who had established that for every $\varepsilon > 0$ there exists a positive constant C such that $V(x) < Cx^{\varepsilon}$.

All the results that I have indicated about the problem of the existence of odd perfect numbers represent a considerable amount of work, sometimes difficult and delicate. Yet I believe the problem stands like an unconquerable fortress. For all that is known, it would be almost by luck that an odd perfect number would be found. On the other hand, nothing that has been proved is promising to show that odd perfect numbers do not exist. New ideas are required.

I wish to conclude this overview of perfect numbers with the following results of Sinha (1974)—the proof is elementary and should be an amusing exercise (just get your pencil ready!): 28 is the only even perfect number that is of the form $a^n + b^n$ with $n \geq 2$, and $\gcd(a,b) = 1$. It is also the only even perfect number of the form $a^n + 1$, with $n \geq 2$. And finally, there is no even perfect number of the form

$$a^{n^{n^{\cdot^{\cdot^{n}}}}} + 1$$

with $n \geq 2$ and at least two exponents n.

Looking back, perfect numbers are defined by comparing N with $\sigma(N)$, the sum of its divisors. Demanding just that N divides $\sigma(N)$ leads to the *multiply perfect numbers*. Numbers N with $2N < \sigma(N)$ are called *abundant*, while those with $2N \geq \sigma(N)$ are called *deficient*.

Let $s(N) = \sigma(N) - N$, the sum of aliquot parts of N, that is, the sum of proper divisors of N. Since some numbers are abundant and others are deficient, it is natural to iterate the process of getting $s(N)$, namely, to build the sequence $s(N)$, $s^2(N)$, $s^3(N), \dots$, where $s^k(N) = s\big(s^{k-1}(N)\big)$. This leads to many fascinating questions, as they are described in Guy's book. Because of space limitations, I am forced to abstain from discussing these matters.

VIII   Pseudoprimes

In this section I shall consider composite numbers having a property which one would think that only prime numbers possess.

A   Pseudoprimes in Base 2 (psp)

A problem, commonly attributed to the ancient Chinese, was to ascertain whether a natural number n must be a prime if it satisfies the congruence

$$2^n \equiv 2 \pmod{n}.$$

On this subject, there are legends and speculations. One should be prudent before making preemptory statements. In view of what one believes to be the knowledge about numbers in ancient China, it seems difficult to conceive that such a question could even be formulated. Siu Man-Keung, a mathematician from Hong Kong interested in the history of mathematics, wrote to me:

> This myth originated in a paper by J.H. Jeans, in the *Messenger of Mathematics*, 27, 1897/8, who wrote that "a paper found among those of the late Sir Thomas Wade and dating from the time of Confucius" contained the theorem that $2^n \equiv 2 \pmod{n}$ holds if and only if n is a prime number. However, in a footnote to his monumental work *Science and Civilisation in China*, Vol. 3, Chap. 19 (Mathematics), J. Needham dispels Jeans' assertion, which is due to an erroneous translation of a passage of the famous book *The Nine Chapters of Mathematical Art.*

This mistake has been perpetuated by several Western scholars. In Dickson's *History of the Theory of Numbers*, Vol. I, p. 91, it is quoted that Leibniz believed to have proved that the so-called Chinese congruence indicated above implies that n is prime. The story is also repeated, for example, in Honsberger's very nicely written chapter "An Old Chinese Theorem and Pierre de Fermat" in his book *Mathematical Gems*, Vol. I, (1973).

There is now a better founded version of the events. In a more recent letter (February 1992), Siu wrote:

I have just seen the doctoral thesis, written in Chinese, of Han Qi, on the mathematics in the Qing period, entitled *Transmission of Western Mathematics during the Kangxi Kingdom and its Influence Over Chinese Mathematics*, Beijing, 1991. The author points out new evidence concerning "the old Chinese theorem". According to Han, this "theorem" is due to Li Shan-Lan (1811–1882), a well-known mathematician of the Qing period (thus the statement is not so old). Li mentioned his criterion to Alexander Wylie, who was his collaborator in the translation of Western texts. Wylie, who probably did not understand mathematics, presented Li's criterion in a note "A Chinese theorem" to the journal *Notes and Queries on China*, Hong Kong, 1869 (1873).

In the succeeding months, at least four readers have written comments on the work of Li; one of the readers pointed out that Li's statement was wrong. Among the readers there was a certain J. von Gumpach, a German who later became a colleague of Li in Beijing. Apparently, Gumpach told Li of his mistake. As a result, in a later publication on number theory (1872), Li Shan-Lan deleted any reference to his criterion. However, in 1882, Hua Heng-Fang, another well-known mathematician of the Qing period, published a treatise on numbers in which he included Li's criterion as if it were correct. This might help to explain why the Western historians of Chinese mathematics were led to think that the criterion might be an old Chinese theorem. Han Qi has announced that he will publish an article on this question, with more details.

I take this opportunity to thank Siu Man-Keung for this well-founded and interesting information.

Concerning the works of Li Shan-Lan you may wish to consult the book of Li Yan and Du Shiran, in an English translation of 1987.

After these comments of historical character, I return to the problem concerning the congruence $2^n \equiv 2 \pmod{n}$, which might be appropriately called, if not as a joke, the "pseudo-Chinese congruence on pseudoprimes".

The first counterexample to the conjecture was obtained in 1819, so much earlier than the events in China. Sarrus showed that $2^{341} \equiv 2$ (mod 341), yet $341 = 11 \times 31$ is a composite number. In particular, a crude converse of Fermat's little theorem is false.

Other composite numbers with this property are, for example: 561, 645, 1105, 1387, 1729, 1905.

A composite number n satisfying the congruence $2^{n-1} \equiv 1$ (mod n) is called a *pseudoprime*, or also a *Poulet number* since that was the focus of his attention. In particular, Poulet computed, as early as 1926, a table of pseudoprimes up to 5×10^7, and in 1938 up to 10^8; see references in Chapter 4.

Every pseudoprime n is odd and also satisfies the congruence $2^n \equiv 2$ (mod n); conversely, every odd composite number satisfying this congruence is a pseudoprime.

Clearly, every odd prime number satisfies the above congruence, so if $2^{n-1} \not\equiv 1$ (mod n), then n must be composite. This is useful as a first step in testing primality.

In order to know more about primes, it is natural to study the integers for which $2^{n-1} \equiv 1$ (mod n).

Suppose I would like to write a chapter about pseudoprimes for the *Guinness Book of Records*. How would I organize it?

The natural questions should be basically the same as those for prime numbers. For example: How many pseudoprimes are there? Can one tell whether a number is a pseudoprime? Are there ways of generating pseudoprimes? How are the pseudoprimes distributed?

As it turns out, not surprisingly, there are infinitely many pseudoprimes, and there are many ways to generate infinite sequences of pseudoprimes.

The simplest proof was given in 1903 by Malo, who showed that if n is a pseudoprime, and if $n' = 2^n - 1$, then n' is also a pseudoprime. Indeed, n' is obviously composite, because if $n = ab$ with $1 < a$, $b < n$, then

$$2^n - 1 = (2^a - 1)\big(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\big).$$

Also n divides $2^{n-1} - 1$, hence n divides $2^n - 2 = n' - 1$; so $n' = 2^n - 1$ divides $2^{n'-1} - 1$.

In 1904, Cipolla gave another proof, using the Fermat numbers:

If $m > n > \cdots > s > 1$ are integers and N is the product of the Fermat numbers $N = F_m F_n \cdots F_s$, then N is a pseudoprime

if and only if $2^s > m$. Indeed, the order of 2 modulo N is 2^{m+1}, which is equal to the least common multiple of the orders 2^{m+1}, $2^{n+1}, \dots, 2^{s+1}$ of 2 modulo each factor F_m, $F_n, \dots, F_s$ of N. Thus $2^{N-1} \equiv 1 \pmod{N}$ if and only if $N-1$ is divisible by 2^{m+1}. But $N-1 = F_m F_n \cdots F_s - 1 = 2^{2^s} Q$, where Q is an odd integer. Thus, the required condition is $2^s > m$. □

As it was indicated in Chapter 1, the Fermat numbers are pairwise relatively prime, so the above method leads to pairwise relatively prime pseudoprimes. One can also obtain pseudoprimes having an arbitrarily large number of prime factors.

Cipolla presented another method that will be described below.

In 1936, Lehmer found a very simple method to generate infinitely many pseudoprimes, each one being the product of two distinct primes p, q. Namely, let $k \geq 5$ be an arbitrary odd integer, let p be a primitive prime factor of $2^k - 1$, and let q be a primitive prime factor of $2^k + 1$. Then pq is a pseudoprime. Thus, for every $m \geq 1$ there exist at least m pseudoprimes $n = pq$ such that

$$ n \leq \left(2^{2m+3} - 1\right) \left(\frac{2^{2m+3} + 1}{3}\right) = \frac{4^{2m+3} - 1}{3}. $$

There also exist even composite integers satisfying the congruence $2^n \equiv 2 \pmod{n}$—they may be called *even pseudoprimes*. The smallest one is $m = 2 \times 73 \times 1103 = 161038$, discovered by Lehmer in 1950. In 1951, Beeger showed the existence of infinitely many even pseudoprimes; each one must have at least two odd prime factors.

How "far" are pseudoprimes from being primes? From Cipolla's result, there are pseudoprimes with arbitrarily many prime factors. This is not an accident. In fact, in 1949 Erdös proved that for every $k \geq 2$ there exist infinitely many pseudoprimes, which are the product of exactly k distinct primes.

In 1936, Lehmer gave criteria for the product of two or three distinct odd primes to be a pseudoprime: $p_1 p_2$ is a pseudoprime if and only if the order of 2 modulo p_2 divides $p_1 - 1$ and the order of 2 modulo p_1 divides $p_2 - 1$. If $p_1 p_2 p_3$ is a pseudoprime, then the least common multiple of $\operatorname{ord}(2 \bmod p_1)$ and $\operatorname{ord}(2 \bmod p_2)$ divides $p_3(p_1 + p_2 - 1) - 1$.

Here is an open question: Are there infinitely many integers $n > 1$ such that $2^{n-1} \equiv 1 \pmod{n^2}$? This is equivalent to each of the following problems (see Rotkiewicz, 1965):

Are there infinitely many pseudoprimes that are squares?

Are there infinitely many primes p such that $2^{p-1} \equiv 1 \pmod{p^2}$?

This congruence was already encountered in the question of square factors of Fermat numbers and Mersenne numbers. I shall return to primes of this kind in Chapter 5, Section III.

On the other hand, a pseudoprime need not be square-free. The smallest such examples are $1\,194\,649 = 1093^2$, $12\,327\,121 = 3511^2$, $3\,914\,864\,773 = 29 \times 113 \times 1093^2$.

B   Pseudoprimes in Base a ($\mathrm{psp}(a)$)

It is also useful to consider the congruence $a^{n-1} \equiv 1 \pmod{n}$, for $a > 2$. If n is a prime and $1 < a < n$, then the above congruence holds necessarily. So, if, for example, $2^{n-1} \equiv 1 \pmod{n}$, but, say, $3^{n-1} \not\equiv 1 \pmod{n}$, then n is not a prime.

This leads to the more general study of the *pseudoprimes in base* a (or a-*pseudoprimes*) which are the composite integers $n > a$ such that $a^{n-1} \equiv 1 \pmod{n}$.

In 1904, Cipolla also indicated how to obtain a-pseudoprimes. Let $a \geq 2$, let p be any odd prime such that p does not divide $a(a^2 - 1)$. Let

$$n_1 = \frac{a^p - 1}{a - 1}, \quad n_2 = \frac{a^p + 1}{a + 1}, \quad n = n_1 n_2;$$

then n_1 and n_2 are odd and n is composite. Since $n_1 \equiv 1 \pmod{2p}$ and $n_2 \equiv 1 \pmod{2p}$, then $n \equiv 1 \pmod{2p}$. From $a^{2p} \equiv 1 \pmod{n}$ it follows that $a^{n-1} \equiv 1 \pmod{n}$, so n is an a-pseudoprime.

Since there exist infinitely many primes, then there also exist infinitely many a-pseudoprimes (also when $a > 2$).

There are other methods in the literature to produce very quickly increasing sequences of a-pseudoprimes.

For example, Crocker proceeded as follows in 1962. Let a be even, but not of the form 2^{2^r}, with $r \geq 0$. Then, for every $n \geq 1$, the number $a^{a^n} + 1$ is an a-pseudoprime.

In 1948, Steuerwald established the following infinite sequence of a-pseudoprimes. Let n be an a-pseudoprime, which is prime to $a - 1$. For example, for a prime q, put $a = q + 1$ and let p be a prime such

that $p > a^2 - 1$; as in the Cipolla construction, let

$$n_1 = \frac{a^p - 1}{a - 1} \equiv a^{p-1} + a^{p-2} + \cdots + a + 1 \equiv p \pmod{q},$$

$$n_2 = \frac{a^p + 1}{a + 1} \equiv a^{p-1} - a^{p-2} + \cdots + a^2 - a + 1 \equiv 1 \pmod{q},$$

so $n = n_1 n_2 \equiv p \pmod{q}$. Let now $f(n) = (a^n - 1)/(a - 1) > n$. Then $f(n)$ is also an a-pseudoprime. Indeed,

$$f(n) = \frac{a^{n_1 n_2} - 1}{a^{n_2} - 1} \times \frac{a^{n_2} - 1}{a - 1}$$

is composite. Since n is prime to $a - 1$ and $a^{n-1} \equiv 1 \pmod{n}$, then n divides $(a^n - a)/(a - 1) = f(n) - 1$. Thus $f(n)$ divides $a^n - 1$, which divides $a^{f(n)-1} - 1$, hence $f(n)$ is an a-pseudoprime. The process may be iterated, noting that $f(n)$ is prime to $a - 1$:

$$f(n) = \frac{[(a - 1) + 1]^n - 1}{a - 1} = (a - 1)^{n-1} + \binom{n}{1}(a - 1)^{n-2}$$

$$+ \cdots + \binom{n}{n-2}(a - 1) + n \equiv n \pmod{a - 1},$$

so $f(n)$ is an a-pseudoprime that is prime to $a - 1$. This process leads to an infinite increasing sequence of a-pseudoprimes $n < f(n) < f(f(n)) < f(f(f(n))) < \cdots$, which grows as n, a^n, a^{a^n} $a^{a^{a^n}}, \ldots$. The method of Lehmer indicated above, applied to binomials $a^k - 1$ and $a^k + 1$, produces a-pseudoprimes which are the product of two distinct prime factors.

From these considerations it follows that it is futile to wish to discover the largest a-pseudoprime.

In 1958, Schinzel showed that for every $a \geq 2$, there exist infinitely many pseudoprimes in base a that are products of two distinct primes.

In 1971, in his thesis, Lieuwens extended simultaneously this result of Schinzel and Erdös' result about pseudoprimes in base 2: for every $k \geq 2$ and $a > 1$, there exist infinitely many pseudoprimes in base a, which are products of exactly k distinct primes.

In 1972, Rotkiewicz showed that if $p \geq 2$ is a prime not dividing $a \geq 2$, then there exist infinitely many pseudoprimes in base a that are multiples of p; the special case when $p = 2$ dates back to 1959, also by Rotkiewicz.

It may occur that a number is a pseudoprime for different bases, like 561 for the bases 2, 5, 7. Indeed, Baillie & Wagstaff and Monier showed independently, in 1980, the following result: Let n be a composite number, and let $B_{\mathrm{psp}}(n)$ be the number of bases a, $1 < a < n$, with $\gcd(a, n) = 1$, for which n is an a-pseudoprime. Then

$$B_{\mathrm{psp}}(n) = \left\{ \prod_{p \mid n} \gcd(n-1, p-1) \right\} - 1.$$

It follows that if n is an odd composite number, which is not a power of 3, then n is a pseudoprime for at least two bases a, $1 < a \le n - 1$.

It will be seen in Section IX that there exist composite numbers n, which are pseudoprimes for all bases a, $1 < a < n$, with $\gcd(a, n) = 1$.

Here is a table, from the paper by Pomerance, Selfridge & Wagstaff (1980), which gives the smallest pseudoprimes for various bases, or simultaneous bases.

Table 10.   Smallest pseudoprimes for several bases

Bases	Smallest psp
2	$341 = 11 \times 31$
3	$91 = 7 \times 13$
5	$217 = 7 \times 31$
7	$25 = 5 \times 5$
2, 3	$1105 = 5 \times 13 \times 17$
2, 5	$561 = 3 \times 11 \times 17$
2, 7	$561 = 3 \times 11 \times 17$
3, 5	$1541 = 23 \times 67$
3, 7	$703 = 19 \times 37$
5, 7	$561 = 3 \times 11 \times 17$
2, 3, 5	$1729 = 7 \times 13 \times 19$
2, 3, 7	$1105 = 5 \times 13 \times 17$
2, 5, 7	$561 = 3 \times 11 \times 17$
3, 5, 7	$29341 = 13 \times 37 \times 61$
2, 3, 5, 7	$29341 = 13 \times 37 \times 61$

As I have said, if there exists a such that $1 < a < n$ and $a^{n-1} \not\equiv 1$ $(\mathrm{mod}\ n)$, then n is composite, but not conversely. This gives therefore

a very practical way to ascertain that many numbers are composite. There are other congruence properties, similar to the above, which give also easy methods to discover that certain numbers are composite.

I shall describe several of these properties; their study has been justified by the problem of primality testing. As a matter of fact, without saying it explicitly, I have already considered these properties in Sections III and V. First, there are properties about the congruence $a^m \equiv 1 \pmod{n}$, which lead to the Euler a-pseudoprimes and strong a-pseudoprimes. In another section, I will examine the Lucas pseudoprimes, which concern congruence properties satisfied by terms of Lucas sequences.

C   EULER PSEUDOPRIMES IN BASE a (epsp(a))

According to Euler's congruence for the Legendre symbol, if $a \geq 2$, p is a prime and p does not divide a, then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

This leads to the notion of an *Euler pseudoprime in base a* (epsp(a)), proposed by Shanks in 1962. These are odd composite numbers n, such that $\gcd(a, n) = 1$ and the Jacobi symbol satisfies the congruence

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}.$$

Clearly, every epsp(a) is an a-pseudoprime.

There are many natural questions about epsp(a) which I enumerate now:

(e1) Are there infinitely many epsp(a), for each a?

(e2) Are there epsp(a) with arbitrary large number of distinct prime factors, for each a?

(e3) For every $k \geq 2$ and base a, are there infinitely many epsp(a), which are equal to the product of exactly k distinct prime factors?

(e4) Can an odd composite number be an epsp(a) for every possible a, $1 < a < n$, $\gcd(a, n) = 1$?

(e5) For how many bases a, $1 < a < n$, $\gcd(a, n) = 1$, can the number n be an $\mathrm{epsp}(a)$?

In 1986, Kiss, Phong & Lieuwens showed that given $a \geq 2$, $k \geq 2$, and $d \geq 2$, there exist infinitely many $\mathrm{epsp}(a)$, which are the product of k distinct primes and are congruent to 1 modulo d.

This gives a strong affirmative answer to (e3), and therefore also to (e2) and (e1).

In 1976, Lehmer showed that if n is odd composite, then it cannot be an $\mathrm{epsp}(a)$, for every a, $1 < a < n$, $\gcd(a, n) = 1$. So the answer to (e4) is negative.

In fact, more is true, as shown by Solovay & Strassen in 1977: a composite integer n can be an Euler pseudoprime for at most $\frac{1}{2}\varphi(n)$ bases a, $1 < a < n$, $\gcd(a, n) = 1$. This gives an answer to question (e5). The proof is immediate, noting that the residue classes $a \bmod n$, for which $(a \mid n) \equiv a^{(n-1)/2} \pmod{n}$ form a subgroup of $(\mathbb{Z}/n)^{\times}$ (group of invertible residue classes modulo n), which is a proper subgroup (by Lehmer's result); hence it has at most $\frac{1}{2}\varphi(n)$ elements—by dear old Lagrange's theorem.

Let n be an odd composite integer. Denote by $B_{\mathrm{epsp}}(n)$ the number of bases a, $1 < a < n$, $\gcd(a, n) = 1$, such that n is an $\mathrm{epsp}(a)$. Monier showed in 1980 that

$$B_{\mathrm{epsp}}(n) = \delta(n) \prod_{p \mid n} \gcd\left(\frac{n-1}{2}, p-1\right) - 1.$$

Here

$$\delta(n) = \begin{cases} 2 & \text{if } v_2(n) - 1 = \min_{p \mid n}\{v_2(p-1)\}, \\ \frac{1}{2} & \text{if there exists a prime } p \text{ dividing } n \text{ such that} \\ & v_p(n) \text{ is odd and } v_2(p-1) < v_2(n-1), \\ 1 & \text{otherwise,} \end{cases}$$

and for any integer m and prime p, $v_p(m)$ denotes the exponent of p in the factorization of m, that is, the p-adic value of m.

D   STRONG PSEUDOPRIMES IN BASE a $(\mathrm{spsp}(a))$

A related property is the following: Let n be an odd composite integer, let $n - 1 = 2^s d$, with d odd and $s \geq 1$; let a be such that $1 < a < n$, $\gcd(a, n) = 1$.

Then n is called a *strong pseudoprime in base a* ($\mathrm{spsp}(a)$) if $a^d \equiv 1$ (mod n) or $a^{2^r d} \equiv -1$ (mod n) for some r, $0 \le r < s$.

Note that if n is a prime, then it satisfies the above condition for every a, $1 < a < n$, $\gcd(a, n) = 1$.

Selfridge showed (see the proof in Williams' paper, 1978) that every $\mathrm{spsp}(a)$ is an $\mathrm{epsp}(a)$. There are partial converses.

By Malm (1977): if $n \equiv 3$ (mod 4) and n is an $\mathrm{epsp}(a)$, then n is a $\mathrm{spsp}(a)$.

By Pomerance, Selfridge & Wagstaff (1980): if n is odd, $(a \mid n) = -1$ and n is an $\mathrm{epsp}(a)$, then n is also a $\mathrm{spsp}(a)$. In particular, if $n \equiv 5$ (mod 8) and n is an $\mathrm{epsp}(2)$, then it is a $\mathrm{spsp}(2)$.

Concerning the strong pseudoprimes, I may ask questions (s1)–(s5), analogous to the questions about Euler pseudoprimes posed in Section VIII, C.

In 1980, Pomerance, Selfridge & Wagstaff proved that for every base $a > 1$, there exist infinitely many $\mathrm{spsp}(a)$, and this answers in the affirmative question (s1), as well as (e1). I shall say more about this in the study of the distribution of pseudoprimes (Chapter 4, Section VI).

For base 2, it is possible to give infinitely many $\mathrm{spsp}(2)$ explicitly, as I indicate now.

If n is a $\mathrm{psp}(2)$, then $2^n - 1$ is a $\mathrm{spsp}(2)$. Since there are infinitely many $\mathrm{psp}(2)$, this gives explicitly infinitely many $\mathrm{spsp}(2)$; among these are all composite Mersenne numbers. It is also easy to see that if a Fermat number is composite, then it is a $\mathrm{spsp}(2)$.

Similarly, since there exist pseudoprimes with arbitrarily large numbers of distinct prime factors, then (s2), as well as (e2), have a positive answer; just note that if $p_1, p_2, \ldots, p_k$ divide the pseudoprime n, then $2^{p_i} - 1$ $(i = 1, \ldots, k)$ divides the $\mathrm{spsp}(2)$ $2^n - 1$.

In virtue of Lehmer's negative answer to (e4) and Selfridge's result, then clearly (s4) has also a negative answer. Very important—as I shall indicate later, in connection with the Monte Carlo primality testing methods—is the next theorem by Rabin, corresponding to Solovay & Strassen's result for Euler pseudoprimes. And it is tricky to prove:

If $n > 4$ is composite, there are at least $3(n - 1)/4$ integers a, $1 < a < n$, for which n is not a $\mathrm{spsp}(a)$. So, the number of bases a, $1 < a < n$, $\gcd(a, n) = 1$, for which an odd composite integer is $\mathrm{spsp}(a)$, is at most $(n - 1)/4$. This answers question (s5).

Monier (1980) has also determined a formula for the number $B_{\mathrm{spsp}}(n)$, of bases a, $1 < a < n$, $\gcd(a, n) = 1$, for which the odd composite integer n is $\mathrm{spsp}(a)$. Namely:

$$B_{\mathrm{spsp}}(n) = \left(1 + \frac{2^{\omega(n)\nu(n)} - 1}{2^{\omega(n)} - 1}\right)\left(\prod_{p|n} \gcd(n^*, p^*)\right) - 1,$$

where

$$
\begin{aligned}
\omega(n) =&\ \text{number of distinct prime factors of } n, \\
\nu(n) =&\ \min_{p|n}\left\{v_2(p-1)\right\}, \\
v_p(m) =&\ \text{exponent of } p \text{ in the factorization of } m \\
&\ (\text{any natural number}), \\
m^* =&\ \text{largest odd divisor of } m - 1.
\end{aligned}
$$

Just for the record, the smallest $\mathrm{spsp}(2)$ is $2047 = 23 \times 89$. It is interesting and also useful to know the smallest strong pseudoprimes to several bases simultaneously. Their knowledge is used in strong primality testing.

Given $k \geq 1$, denote by t_k the smallest integer which is a strong pseudoprime for the bases $p_1 = 2$, $p_2 = 3$, ... , p_k, simultaneously. Then the calculations of Pomerance, Selfridge & Wagstaff (1980), extended by Jaeschke (1993), provide the following values:

$$
\begin{aligned}
t_2 &= 1\,373\,653 = 829 \times 1657, \\
t_3 &= 25\,326\,001 = 2251 \times 11251, \\
t_4 &= 3\,215\,031\,751 = 151 \times 751 \times 28351, \\
t_5 &= 2\,152\,302\,898\,747 = 6763 \times 10627 \times 29947, \\
t_6 &= 3\,474\,749\,660\,383 = 1303 \times 16927 \times 157543, \\
t_7 &= t_8 = 341\,550\,071\,728\,321 = 10670053 \times 32010157.
\end{aligned}
$$

Jaeschke's work also showed that there are only 101 numbers below 10^{12} which are strong pseudoprimes for the bases 2, 3, and 5, simultaneously. Since their complete list is fairly large, I reproduce only the one published by the three Knights of Numerology, which is restricted to numbers less than 25×10^9.

Table 11.

Numbers less than 25×10^9, which are spsp in bases 2, 3, 5

Number	psp to base			Factorization
	7	11	13	
25 326 001	no	no	no	2251×11251
161 304 001	no	spsp	no	7333×21997
960 946 321	no	no	no	11717×82013
1 157 839 381	no	no	no	24061×48121
3 215 031 751	spsp	psp	psp	$151 \times 751 \times 28351$
3 697 278 427	no	no	no	30403×121609
5 764 643 587	no	no	spsp	37963×151849
6 770 862 367	no	no	no	41143×164569
14 386 156 093	psp	psp	psp	$397 \times 4357 \times 8317$
15 579 919 981	psp	spsp	no	88261×176521
18 459 366 157	no	no	no	67933×271729
19 887 974 881	psp	no	no	81421×244261
21 276 028 621	no	psp	psp	103141×206281

To this table, I add the list of pseudoprimes up to 25×10^9 which are not square-free and their factorizations:

$$1\,194\,649 = 1093^2,$$
$$12\,327\,121 = 3511^2,$$
$$3\,914\,864\,773 = 29 \times 113 \times 1093^2,$$
$$5\,654\,273\,717 = 1093^2 \times 4733,$$
$$6\,523\,978\,189 = 43 \times 127 \times 1093^2,$$
$$22\,178\,658\,685 = 5 \times 47 \times 79 \times 1093^2.$$

With the exception of the last two, the numbers in the above list are strong pseudoprimes.

Note that the only prime factors to the square are 1093 and 3511. The occurrence of these numbers will be explained in Chapter 5, Section III.

IX   Carmichael Numbers

In a short article which remained unnoticed, Korselt considered in 1899 a more rare kind of numbers; they were also introduced independently by Carmichael in 1912, who first studied their properties. Since his article was noted, such numbers came to be called *Carmichael numbers.* By definition, they are the composite numbers n such that $a^{n-1} \equiv 1 \pmod{n}$ for every integer a, $1 < a < n$, such that a is relatively prime to n. The smallest Carmichael number is $561 = 3 \times 11 \times 17$.

I shall now indicate a characterization of Carmichael numbers. Recall that I have introduced, in Section II, Carmichael's function $\lambda(n)$, which is the maximum of the orders of $a \bmod n$, for every a, $1 \leq a < n$, $\gcd(a, n) = 1$; in particular, $\lambda(n)$ divides $\varphi(n)$.

Carmichael showed that n is a Carmichael number if and only if n is composite and $\lambda(n)$ divides $n - 1$. (It is the same as saying that if p is any prime dividing n, then $p - 1$ divides $n - 1$.)

It follows that every Carmichael number is odd and is the product of three or more distinct prime numbers.

Explicitly, if $n = p_1 p_2 \cdots p_r$ (product of distinct primes), then n is a Carmichael number if and only if $p_i - 1$ divides $(n/p_i) - 1$ (for $i = 1, 2, \ldots, r$). Therefore, if n is a Carmichael number, then also $a^n \equiv a \pmod{n}$, for every integer $a \geq 1$.

Schinzel noted in 1959 that for every $a \geq 2$ the smallest pseudo-prime m_a in base a satisfies necessarily $m_a \leq 561$. Moreover, there exists a such that $m_a = 561$. Explicitly, let p_i ($i = 1, \ldots, s$) be the primes such that $2 < p_i < 561$; for each p_i let e_i be such that $p_i^{e_i} < 561 < p_i^{e_i+1}$; let g_i be a primitive root modulo $p_i^{e_i}$, and by the Chinese remainder theorem, let a be such that $a \equiv 3 \pmod{4}$ and $a \equiv g_i \pmod{p_i^{e_i}}$ for $i = 1, \ldots, s$. Then $m_a = 561$.

Carmichael and Lehmer determined the smallest Carmichael numbers:

$561 = 3 \times 11 \times 17$	$15841 = 7 \times 31 \times 73$	$101101 = 7 \times 11 \times 13 \times 101$
$1105 = 5 \times 13 \times 17$	$29341 = 13 \times 37 \times 61$	$115921 = 13 \times 37 \times 241$
$1729 = 7 \times 13 \times 19$	$41041 = 7 \times 11 \times 13 \times 41$	$126217 = 7 \times 13 \times 19 \times 73$
$2465 = 5 \times 17 \times 29$	$46657 = 13 \times 37 \times 97$	$162401 = 17 \times 41 \times 233$
$2821 = 7 \times 13 \times 31$	$52633 = 7 \times 73 \times 103$	$172081 = 7 \times 13 \times 31 \times 61$
$6601 = 7 \times 23 \times 41$	$62745 = 3 \times 5 \times 47 \times 89$	$188461 = 7 \times 13 \times 19 \times 109$
$8911 = 7 \times 19 \times 67$	$63973 = 7 \times 13 \times 19 \times 37$	$252601 = 41 \times 61 \times 101$
$10585 = 5 \times 29 \times 73$	$75361 = 11 \times 13 \times 17 \times 31$	

I consider now the following questions, which are of course closely related:

(1) Are there infinitely many Carmichael numbers?

(2) Given $k \geq 3$, are there infinitely many Carmichael numbers having exactly k prime factors?

The first problem was solved in 1992, in the affirmative, in a brilliant paper by Alford, Granville & Pomerance that appeared in 1994; see also the expository paper by Pomerance (1993).

It is believed that the answer to the second question is also affirmative, but this has yet to be established. For example, it is not even known if there exist infinitely many Carmichael numbers, which are products of exactly three primes. In this respect, there is a result of Duparc (1952) (see also Beeger, 1950):

For every $r \geq 3$, there exist only finitely many Carmichael numbers with r prime factors, of which the smallest $r - 2$ factors are given in advance. I shall return to these questions in Chapter 4.

In 1939, Chernick gave the following method to obtain Carmichael numbers. Let $m \geq 1$ and

$$M_3(m) = (6m + 1)(12m + 1)(18m + 1).$$

If m is such that all three factors above are prime, then $M_3(m)$ is a Carmichael number. This yields Carmichael numbers with three prime factors. But obviously we do not know if there exist infinitely many integers m having that property.

Similarly, if $k \geq 4$, $m \geq 1$, let

$$M_k(m) = (6m + 1)(12m + 1) \prod_{i=1}^{k-2} (9 \times 2^i m + 1).$$

If m is such that all k factors are prime numbers and, moreover, 2^{k-4} divides m, then $M_k(m)$ is a Carmichael number with k prime factors.

This method, or variants of it, have been used to produce Carmichael numbers which are large or have many prime factors.

I note: Wagstaff in 1980 (321 digits), Atkin in 1980 (370 digits), Woods & Huenemann in 1982 (432 digits), Dubner in 1985 (1057 digits), Dubner in 1989 (3710 digits).

While these examples have only a few prime factors, Yorinaga (1978) determined Carmichael numbers with up to 15 prime factors.

The search for large Carmichael numbers with many prime factors continued. In 1994 (published in 1996), Löh & Niebuhr constructed a Carmichael number with 16142049 digits and 1101518 prime factors.

RECORD

The largest known Carmichael number was determined by W.R. Alford and J. Grantham in 1998; it has 20163700 digits and 1371497 prime factors. Also, this number has the following additional property: for every k with $62 \leq k \leq 1371435$ it is divisible by a Carmichael number having exactly k prime factors.

This unpublished record was kindly communicated to me by the authors.

Stimulated by a deeper understanding of this kind of computations, Alford, Granville & Pomerance (1994) established the thruth of this old conjecture: There exist infinitely many Carmichael numbers.

Concerning the calculation of Carmichael numbers, Pinch has produced, in 1998, the complete list of these numbers up to 10^{16}. I shall discuss his findings in Chapter 4, Section VI, B.

The distribution of Carmichael numbers will be studied in Chapter 4, Section VIII.

ADDENDUM ON KNÖDEL NUMBERS

For every $k \geq 1$, let C_k be the set of all composite integers $n > k$ such that if $1 < a < n$ and $\gcd(a, n) = 1$, then $a^{n-k} \equiv 1 \pmod{n}$.

Thus, C_1 is the set of Carmichael numbers. For $k \geq 2$, the numbers C_k were considered by Knödel in 1953. Even before it was proved that there exist infinitely many Carmichael numbers, Mąkowski proved in 1962:

For each $k \geq 2$, the set C_k is infinite.

Proof. For every a, $1 < a < k$, $\gcd(a, k) = 1$, let r_a be the order of a modulo k. Let $r = \prod r_a$ (product for all a as above). So $a^r \equiv 1 \pmod{k}$.

There exist infinitely many primes p such that $p \equiv 1 \pmod{r}$; see Chapter 4, Section IV, for a proof of this very useful theorem. For each such $p > k$, write $p - 1 = hr$, and let $n = kp$. Then $n \in C_k$.

Indeed, let $1 \leq a < n$, $\gcd(a, n) = 1$, so $\gcd(a, k) = 1$; hence

$$a^{n-k} = a^{k(p-1)} = a^{khr} \equiv 1 \pmod{k},$$

$$a^{n-k} = a^{k(p-1)} \equiv 1 \pmod{p}.$$

Since $p \nmid k$, then $a^{n-k} \equiv 1 \pmod{n}$, showing that $n = kp$ is in C_k.
□

It follows from the above proof that if $k = 2$, then $2p \in C_2$ for every prime $p > 2$. If $k = 3$, then $3p \in C_3$ for every prime $p > 3$; this last fact was proved by Morrow in 1951.

X   Lucas Pseudoprimes

In view of the analogy between sequences of binomials $a^n - 1$ $(n \geq 1)$ and Lucas sequences, it is no surprise that pseudoprimes should have a counterpart involving Lucas sequences. For each parameter $a \geq 2$, there were the a-pseudoprimes and their cohort of Euler pseudo-primes and strong pseudoprimes in base a. In this section, to all pairs (P, Q) of nonzero integers will be associated the corresponding Lucas pseudoprimes, the Euler-Lucas pesudoprimes, and the strong Lucas pseudoprimes. Their use will parallel that of pseudoprimes.

Let P, Q be nonzero integers, $D = P^2 - 4Q$ and consider the associated Lucas sequences $(U_n)_{n \geq 0}$, $(V_n)_{n \geq 0}$.

Recall (from Section IV) that if n is an odd prime, then:

(X.1)   If $\gcd(n, D) = 1$, then $U_{n-(D|n)} \equiv 0 \pmod{n}$.

(X.2) $U_n \equiv (D \mid n) \pmod{n}$.

(X.3) $V_n \equiv P \pmod{n}$.

(X.4)   If $\gcd(n, D) = 1$, then $V_{n-(D|n)} \equiv 2Q^{(1-(D/n))/2} \pmod{n}$.

If n is an odd composite number and the congruence (X.1) holds, then n is called a *Lucas pseudoprime* (with the parameters (P, Q)), abbreviated lpsp(P, Q).

It is alright to make such a definition, but do these numbers exist? If so, are they worthwhile to study?

A   Fibonacci Pseudoprimes

To begin, it is interesting to look at the special case of Fibonacci numbers, where $P = 1$, $Q = -1$, $D = 5$. In this situation, it is more appropriate to call *Fibonacci pseudoprimes* the lpsp$(1, -1)$.

The smallest Fibonacci pseudoprimes are $323 = 17 \times 19$ and $377 = 13 \times 29$; indeed, $(5 \mid 323) = (5 \mid 377) = -1$ and it may be calculated that $U_{324} \equiv 0 \pmod{323}$, $U_{378} \equiv 0 \pmod{377}$.

E. Lehmer showed in 1964 that there exist infinitely many Fibonacci pseudoprimes; more precisely, if p is any prime greater than 5, then U_{2p} is a Fibonacci pseudoprime.

Property (X.2) was investigated by Parberry (in 1970) and later by Yorinaga (1976).

Among his several results, Parberry showed that if $\gcd(h, 30) = 1$ and condition (X.2) is satisfied by h, then it is also satisfied by $k = U_h$; moreover, $\gcd(k, 30) = 1$ and, if h is composite, clearly U_h is also composite. This shows that if there exists one composite Fibonacci number U_n such that $U_n \equiv (5 \mid n) \pmod{n}$, then there exist infinitely many such numbers. As I shall say (in a short while) there do exist such Fibonacci numbers.

Actually, this also follows from another result of Parberry: If p is prime and $p \equiv 1$ or $4 \pmod{15}$, then $n = U_{2p}$ is odd composite and it satisfies both properties (X.1) and (X.2). In particular, there are infinitely many Fibonacci pseudoprimes which, moreover, satisfy (X.2). (Here I use the fact—to be indicated later in Chapter 4, Section IV—that there exist infinitely many primes p such that $p \equiv 1 \pmod{15}$, resp. $p \equiv 4 \pmod{15}$.)

If $p \not\equiv 1$ or $4 \pmod{15}$, then (X.2) is not satisfied, as follows from various divisibility properties and congruences indicated in Section IV.

Yorinaga considered the primitive part of the Fibonacci number U_n. If you remember, I have indicated in Section IV that every Fibonacci number U_n (with $n \neq 1, 2, 6, 12$) admits a primitive prime factor p—these are the primes that divide U_n, but do not divide U_d, for every d, $1 < d < n$, d dividing n. Thus $U_n = U_n^* \times U_n'$, where $\gcd(U_n^*, U_n') = 1$ and p divides U_n^* if and only if p is a primitive prime factor of U_n.

Yorinaga showed that if m divides U_n^* (with $n > 5$) then $U_m \equiv (5 \mid m) \pmod{m}$.

According to Schinzel's result (1963), discussed in Section IV, there exist infinitely many integers n such that U_n^* is not a prime. So, Yorinaga's result implies that there exist infinitely many odd composite n such that the congruence (X.2) is satisfied.

Yorinaga published a table of all 109 composite numbers n up to 707000, such that $U_n \equiv (5 \mid n) \pmod{n}$. Some of these numbers also give Fibonacci pseudoprimes, like $n = 4181 = 37 \times 113$, $n = 5777 = 53 \times 109$, and many more. Four of the numbers in the table give pseudoprimes in base 2:

$$219781 = 271 \times 811,$$
$$252601 = 41 \times 61 \times 101,$$
$$399001 = 31 \times 61 \times 211,$$
$$512461 = 31 \times 61 \times 271.$$

Another result of Parberry, later generalized by Baillie & Wagstaff, is the following:

If n is an odd composite number, not a multiple of 5, if congruences (X.1) and (X.2) are satisfied, then

$$\begin{cases} U_{(n-(5|n))/2} \equiv 0 \pmod{n} & \text{if} \quad n \equiv 1 \pmod{4}, \\ V_{(n-(5|n))/2} \equiv 0 \pmod{n} & \text{if} \quad n \equiv 3 \pmod{4}. \end{cases}$$

In particular, since there are infinitely many composite integers n such that $n \equiv 1 \pmod{4}$, then there are infinitely many odd composite integers n satisfying the congruence $U_{(n-(5|n))/2} \equiv 0 \pmod{n}$.

The composite integers n such that $V_n \equiv 1 \pmod{n}$ (where $(V_k)_{k \geq 0}$ is the sequence of Lucas numbers) have also been studied. They have been called *Lucas pseudoprimes*, but this name is used here with a different meaning.

In 1983, Singmaster found the following 25 composite numbers $n < 10^5$ with the above property:

705, 2465, 2737, 3745, 4181, 5777, 6721,
10877, 13201, 15251, 24465, 29281, 34561,
35785, 51841, 54705, 64079, 64681, 67861,
68251, 75077, 80189, 90061, 96049, 97921.

B   Lucas Pseudoprimes ($\mathrm{lpsp}(P,Q)$)

I shall now consider $\mathrm{lpsp}(P,Q)$ associated to arbitrary pairs of parameters (P,Q). To stress the analogy with the pseudoprimes in base a, the discussion should follow the same lines, but it will be clear that much less is known about these numbers. For example, there is no explicit mention of any algorithm to generate infinitely many $\mathrm{lpsp}(P,Q)$, when P, Q are given—except the results mentioned for Fibonacci pseudoprimes.

However, in his thesis in 1971, Lieuwens stated that for every $k \geq 2$, there exist infinitely many Lucas pseudoprimes with given parameters (P,Q), which are the product of exactly k distinct primes.

It is quite normal for an odd integer n to be a Lucas pseudoprime with respect to many different sets of parameters. Let $D \equiv 0$ or 1 (mod 4), let $B_{\mathrm{lpsp}}(n,D)$ denote the number of integers P, $1 \leq P \leq n$, such that there exists Q, with $P^2 - 4Q \equiv D$ (mod n) and n is a $\mathrm{lpsp}(P,Q)$. Baillie & Wagstaff showed in 1980 that

$$B_{\mathrm{lpsp}}(n,D) = \prod_{p|n} \left\{ \gcd\left(n - \left(\frac{D}{n}\right),\, p - \left(\frac{D}{p}\right)\right) - 1 \right\}.$$

In particular, if n is odd and composite, there exists D and, correspondingly, at least three pairs (P,Q), with $P^2 - 4Q = D$ and distinct values of P modulo n, such that n is a $\mathrm{lpsp}(P,Q)$.

Another question is the following: If n is odd, for how many distinct D modulo n, do there exist (P,Q) with $P^2 - 4Q \equiv D$ (mod n), $P \not\equiv 0$ (mod n), and n is a $\mathrm{lpsp}(P,Q)$? Baillie & Wagstaff also discussed this matter when $n = p_1 p_2$, where p_1, p_2 are distinct primes.

C   Euler-Lucas Pseudoprimes ($\mathrm{elpsp}(P,Q)$) and Strong Lucas Pseudoprimes ($\mathrm{slpsp}(P,Q)$)

Let P, Q be given, $D = P^2 - 4Q$, as before. Let n be an odd prime number. If $\gcd(n, QD) = 1$, it was seen in Section V that

(el) $\begin{cases} U_{(n-(D|n))/2} \equiv 0 \quad (\text{mod } n) & \text{when} \quad (Q \mid n) = 1, \\ V_{(n-(D|n))/2} \equiv D \quad (\text{mod } n) & \text{when} \quad (Q \mid n) = -1. \end{cases}$

This leads to the following definition. An odd composite integer n, such that $\gcd(n, QD) = 1$, satisfying the above condition is called a

Euler–Lucas pseudoprime with parameters (P, Q), abbreviated elpsp(P, Q).

Let n be an odd composite integer, with $\gcd(n, D) = 1$, let $n - (D \mid n) = 2^s d$, with d odd, $s \geq 0$. If

$$
\text{(sl)} \quad
\begin{cases}
U_d \equiv 0 \pmod{n}, & \text{or} \\
V_{2^r d} \equiv 0 \pmod{n} & \text{for some } r,\ 0 \leq r < s,
\end{cases}
$$

then n is called a *strong Lucas pseudoprime* with parameters (P, Q), abbreviated slpsp(P, Q). In this case, necessarily, $\gcd(n, Q) = 1$.

If n is an odd prime, and $\gcd(n, QD) = 1$, then n satisfies the congruences (el) and (sl) above. It is also clear that if n is an elpsp(P, Q) and $\gcd(n, Q) = 1$, then n is a lpsp(P, Q).

What are the relations between elpsp(P, Q) and slpsp(P, Q)? Just as in the case of Euler and strong pseudoprimes in base a, Baillie & Wagstaff showed that if n is a slpsp(P, Q), then n is an elpsp(P, Q)—this is the analogue of Selfridge's result.

Conversely, if n is an elpsp(P, Q) and either $(Q \mid n) = -1$ or $n - (D \mid n) \equiv 2 \pmod{4}$, then n is a slpsp(P, Q)—this is the analogue of Malm's result.

If $\gcd(n, Q) = 1$, n is a lpsp(P, Q), $U_n \equiv (D \mid n) \pmod{n}$ and if, moreover, n is an elpsp(P, Q), then n is also a slpsp(P, Q). The special case for Fibonacci numbers was proved by Parberry, as already indicated.

Previously, I mentioned the result of Lehmer, saying that no odd composite number can be an epsp(a), for all possible bases. Here is the analogous result of Williams (1977): Given $D \equiv 0$ or $1 \pmod 4$, if n is an odd composite integer, and $\gcd(n, D) = 1$, there exist P, Q, nonzero integers, with $P^2 - 4Q = D$, $\gcd(P, Q) = 1$, $\gcd(n, Q) = 1$, and such that n is not an elpsp(P, Q).

With the present terminology, I have mentioned already that Parberry had shown, for the Fibonacci sequence, that there exist infinitely many elpsp$(1, -1)$.

This has been improved by Kiss, Phong & Lieuwens (1986): Given (P, Q) such that the sequence $(U_n)_{n \geq 0}$ is nondegenerate (that is, $U_n \neq 0$ for every $n \geq 0$), given $k \geq 2$, there exist infinitely many elpsp(P, Q), each being the product of k distinct primes. Moreover, given also $d \geq 2$, if $D = P^2 - 4Q > 0$, then the prime factors may all be chosen to be of the form $dm + 1$ ($m \geq 1$).

As for Fibonacci numbers, I now consider the congruences (X.2) and also (X.3), (X.4). It may be shown that if $\gcd(n, 2PQD) = 1$ and if n satisfies any two of the congruences (X.1) to (X.4), then it satisfies the other two.

In 1986, Kiss, Phong & Lieuwens extended a result of Rotkiewicz (1973) and proved: Given $P, Q = \pm 1$ (but $(P, Q) \neq (1, 1)$), given $k \geq 2$, $d \geq 2$, there exist infinitely many integers n, which are Euler pseudoprimes in base 2, and which satisfy the congruences (X.1) to (X.4); moreover, each such number n is the product of exactly k distinct primes, all of the form $dm + 1$ (with $m \geq 1$).

D   Carmichael–Lucas Numbers

Following the same line of thought that led from pseudoprimes to Carmichael numbers, it is natural to consider the following numbers.

Given $D \equiv 0$ or $1 \pmod 4$, the integer n is called a *Carmichael–Lucas number* (associated to D), if $\gcd(n, D) = 1$ and for all nonzero relatively prime integers P, Q with $P^2 - 4Q = D$ and $\gcd(n, Q) = 1$, the number is an lpsp(P, Q).

Do such numbers exist? A priori, this is not clear. Of course, if n is a Carmichael–Lucas number associated to $D = 1$, then n is a Carmichael number.

Williams, who began the consideration of Carmichael–Lucas numbers, showed in 1977:

If n is a Carmichael–Lucas number associated to D, then n is the product of $k \geq 2$ distinct primes p_i such that $p_i - (D \mid p_i)$ divides $n - (D \mid n)$.

Note that $323 = 17 \times 19$ is a Carmichael–Lucas number (with $D = 5$); but it cannot be a Carmichael number, because it is the product of only two distinct primes.

Adapting the method of Chernick, it is possible to generate many Carmichael–Lucas numbers. Thus, for example, $1649339 = 67 \times 103 \times 239$ is such a number (with $D = 8$).

XI   Primality Testing and Factorization

I reserve the last section to treat a burning topic, full of tantalizing ideas and the object of intense research, in view of immediate direct applications.

Immediate direct applications of number theory! Who would dream of it, even some 40 years ago? Von Neumann yes, not me, not many people. Poor number theory, the Queen relegated (or raised?) to be the object of a courtship inspired by necessity not by awe.

In recent years, progress on the problems of primality testing and factorization have been swift. More and more deep results of number theory have been invoked. Brilliant brains devised clever procedures, not less brilliant technicians invented tricks, shortcuts to implement the methods in a reasonable time—and thus, a whole new branch of number theory is evolving.

In previous sections of this chapter, I have attempted to develop the foundations needed to present in a lucid way the main procedures for primality testing. But this was doomed to failure. Indeed, with the latest developments I would need, for example, to use facts about the theory of Jacobi sums, algebraic number theory, elliptic curves, abelian varieties, etc. This is far beyond what I intend to discuss. It is more reasonable to assign supplementary reading for those who are avidly interested in the problem. Happily enough, there are now many excellent expository articles and books, which I will recommend at the right moment.

Despite the shortcomings just mentioned, I feel that presenting an overview of the question, even one with gaps, will still be useful. Having apologized, I may now proceed with my incomplete treatment.

First, money: how much it costs to see the magic. Then, I shall discuss more amply primality tests, indicate some noteworthy recent factorizations, to conclude with a quick description of applications to public key cryptography. I will be happy if the presentation which follows will make my reader thirsty. Thirsty to know more about what he has read here, and for this purpose, I recommend the books of Williams (1998) and of Crandall & Pomerance (2001).

A   THE COST OF TESTING

The cost of applying an algorithm to a number N is proportional to the time required and, in turn, it depends on the machine, the program, and the size of the number.

The operations should be counted in an appropriate way, since it is clear that addition or multiplication of very large numbers is more time consuming than if the numbers were small. So, in the last analysis, the cost is proportional to the number of operations with digits—such indivisible operations are called bit operations. Thus, for the calculation, the input is not the integer N, but the number of its digits in some base system, which is then proportional to $\log N$.

The algorithm runs in *polynomial time* if there exists a polynomial $f(X)$ such that, for every N, the time required to perform the algorithm on the number N is bounded by $f(\log N)$. An algorithm, not of polynomial time, whose running time is bounded by $f(N)$ (for every N) where $f(X)$ is a polynomial, is said to have an *exponential* running time, since $N = e^{\log N}$. An algorithm can only be economically justified if it runs in polynomial time.

The theory of complexity of algorithms deals specifically with the determination of bounds for the running time. It is a very elaborate sort of bookkeeping, which requires a careful analysis of the methods involved. Through the discovery of clever tricks, algorithms may sometimes be simplified into others requiring only a polynomial running time.

It may be said that the main problem faced in respect to primality testing (and many other problems) is the following:

Does there exist an algorithm to perform the test, which runs in polynomial time?

This problem has just been solved in the affirmative, as I shall discuss soon at the appropriate place. But first, I will consider other tests for primality, which do not run in polynomial time, and yet are very practical for actual testing.

All this should not be confused with the following.

If a number N is known to be composite, this fact may be proved with only one operation. Indeed, it is enough to produce two numbers a, b, such that $N = ab$, so the number of bit operations required is at most $(\log N)^2$. Paraphrasing Lenstra, it is irrelevant whether a, b were found after consulting a clairvoyant, or after three years of

Sundays, like Cole's factorization of the Mersenne number M_{67}:

$$2^{67} - 1 = 193707721 \times 761838257287.$$

If p is known to be a prime, what is the number of bit operations required to prove it? This is not so easy to answer. In 1975, Pratt showed that it suffices a $C(\log p)^4$ bit operations (where C is a positive constant).

In 1987, Pomerance applied the Hasse-Weil theorem on the number of points on elliptic curves defined modulo some integer n. He was able to show that if p is known to be a prime, then a proof of this fact may be done involving at most $C \log p$ multiplications modulo p. This was better than all the other earlier certification proofs.

B   More Primality Tests

I return once more to primality testing. There are many kinds of tests, and according to the point of view, they may be classified as follows:

$$\begin{cases} \text{Tests for numbers of special forms} \\ \text{Tests for generic numbers} \end{cases}$$

or

$$\begin{cases} \text{Tests with full justification} \\ \text{Tests with justification based on conjectures} \end{cases}$$

or

$$\begin{cases} \text{Deterministic tests} \\ \text{Probabilistic or Monte Carlo tests.} \end{cases}$$

In the sequel, I shall encounter tests of each of the above kinds.

If sufficiently many prime factors of $N-1$ or $N+1$ are known, the tests indicated in Sections III and V run in polynomial time on the number of digits of the input. These are *special purpose* primality tests, each one being very effective for numbers of appropriate form.

In contrast, a *general purpose* primality test is applicable to any number and is not specifically designed to handle more effectively any one kind of number.

The justification of a primality test ought to be based on theorems of number theory. But there are cases where no justification is known without appealing to unproved conjectures, like some form of Riemann's hypothesis.

Many of the tests are deterministic and the steps are all prescribed in advance. In other tests, there are random choices made in some steps during the testing.

When a number N is submitted to a primality test, the desired output is one of the following two answers: "N is a prime," or "N is composite." However, there are tests leading to the following outputs: "N is composite," or "N satisfies a property shared by prime numbers." Since there are measures of probability attached to the test, these are called probabilistic or Monte Carlo tests.

If it has been ascertained that a number N has a high probability of being a prime, it is customary to call such a number a *probable prime.* Of course, it should be borne in mind that a number $N > 1$ is either prime or composite. The designation of "probable prime" reflects the lack of knowledge, at a given moment, of the exact kind of number, prime, or composite.

Once a test is performed and the number is designated to be a prime, often after extensive calculations, usually subjected to the hazards of human or machine errors, it is of the utmost importance to ratify the result obtained. A second or third repetition of the test, preferably performed with different programs and on different machines, giving the same output is reassuring enough—but not a proof that the output is correctly given.

In this respect, the most desirable feature is a certificate of primality, when the number is declared a prime; this certificate would be a proof of primality for the number. — Now I wish to discuss a few—very few—of the methods to test primality.

Trial division

For numbers that are not of a special form, the very naive primality test is by trial division of N by all primes $p < \sqrt{N}$. It will be seen in Chapter 4 that, for any large integer N, the number of primes less than $\sqrt{N}$ is about $2\sqrt{N}/\log N$ (this statement will be made much more precise later on); thus there will be at most $C\sqrt{N}/\log N$ operations (where $C > 0$ is a constant), which tells that the running time could be $C\sqrt{N}/\log N$. So this procedure does not run in polynomial time on the input.

Miller's test

In 1976, Miller proposed a primality test, which was justified using a generalized form of Riemann's hypothesis. I will not explain the

exact meaning of this hypothesis or conjecture, but in Chapter 4, I shall discuss the classical Riemann's hypothesis.

To formulate Miller's test, which involves the congruences used in the definition of strong pseudoprimes, it is convenient to use the terminology introduced by Rabin.

Let N be an integer, $N-1 = 2^s d$, with $s \geq 0$, d odd. Let $1 < a < N$ with $\gcd(a, N) = 1$. Then a is said to be a *witness* for N when $a^d \not\equiv 1 \pmod{N}$ and $a^{2^r d} \not\equiv -1 \pmod{N}$ for every r, $0 \leq r < s$.

If N has a witness, it is composite. If N is composite, if $1 < a < N$, $\gcd(a, N) = 1$, and a is not a witness, then N is a spsp(a). Conversely, if N is odd and N is a spsp(a) then a is not a witness for N.

In this terminology, it suffices to show that no integer a, $1 < a < N$, $\gcd(a, N) = 1$, is a witness, in order to deduce that N is prime. Since N is assumed to be very large, this task is overwhelming! It would be wonderful just to settle the matter by considering small integers a, and checking whether any one is a witness for N. Here is where the generalized Riemann's hypothesis is needed. It was used to show:

Miller's test. *Let N be an odd integer. If there exists a, such that $\gcd(a, N) = 1$, $1 < a < 2(\log N)^2$, which is a witness for N, then N is composite. Otherwise, N is a prime.*

I should add here that for numbers up to 25×10^9, because of the calculations reported in Section VIII, the only composite integer N that is a strong pseudoprime simultaneously to the bases 2, 3, 5, 7, is the number $3\,215\,031\,751$. So if $N < 25 \times 10^9$ is not this number, and 2, 3, 5, 7 are not witnesses, then N is a prime. As shown by Jaeschke (1993), this is also true up to $N < 118\,670\,087\,467$.

This test may be easily implemented on a pocket calculator.

The number of bit operations for testing whether a number is a witness for N is at most $C(\log N)^5$, where C is a positive constant. So, this test runs in polynomial time on the input, provided the generalized Riemann's hypothesis is assumed true.

In 1979, Lenstra published a streamlined version of Miller's test, which he discussed again in his paper of 1982. See also the nice expository paper by Wagon (1986).

The APR test

The primality test devised by Adleman, Pomerance & Rumely (1983), usually called the APR test, represents a breakthrough. To wit:

(i) It is a deterministic general purpose primality test; thus, it is applicable to arbitrary natural numbers N, without requiring the knowledge of factors of $N - 1$ or $N + 1$.

(ii) The running time $t(N)$ is almost polynomial; more precisely, there exist effectively computable constants $0 < C' < C$, such that

$$(\log N)^{C' \log \log \log N} \leq t(N) \leq (\log N)^{C \log \log \log N}.$$

(iii) The test is justified rigorously, and for the first time ever in this domain, it was necessary to appeal to deep results in the theory of algebraic numbers. The test involves calculations with roots of unity and the general reciprocity law for the power residue symbol. (Did you notice that I have not explained these concepts? It is far beyond what I plan to treat.)

Up to 2002, the APR test had the best running time among all deterministic general purpose primality tests.

Soon after its publication, Cohen & Lenstra (1984) modified the APR test, making it more flexible, using Jacobi sums in the proof (instead of the reciprocity law), and having the new test programmed for practical applications. It was the first primality test in existence that could routinely handle numbers of up to 200 decimal digits, the test being executed in about ten minutes, while numbers of up to 100 digits were treated in about 45 seconds.

In 1987, Cohen & Lenstra, Br. (Brother, not Junior), tested a number of 247 digits (a prime factor of $2^{892} + 1$), in about 15 minutes.

A presentation of the APR test was made by Lenstra in the Séminaire Bourbaki, Exposé 576 (1981). It was also discussed in papers of Lenstra (1982) and Nicolas (1984), as well as in the important book by Cohen (1993).

Tests with elliptic curves

In 1986, Atkin presented his own new primality test which used elliptic curves over finite fields, the first test of this kind. It runs

in random polynomial time, it is fully justified, and if the output is "prime", it comes assorted with a list of numbers from which it is easily verified, without performing all the calculations again, that the number is indeed a prime. Such a list of intermediate results is called just a *certificate* for the prime number.

Atkin & Morain (1993) published a long paper devoted to their method, called ECPP ("elliptic curve primality proving"), which is described in its various aspects. The algorithm has been refined by Morain, who succeeded to prove, and to certify, the primality of various interesting numbers having more than 1000 digits. Other, most effective implementations of the test are currently being used.

Due to its complexity, I shall not even try to indicate the basic steps of the ECPP algorithm.

Record

The largest number proved prime by using a general purpose primality test (rigorously justified and applicable to an arbitrary number), is a 5878 digit number $16282536\ldots36478311$, which has the special property that it is preceded by a row of 233821 composite numbers.

The certification of this prime, completed in February 2003, was accomplished by J.L. Gómez Pardo, using the ECPP implementation of M. Martin. The computations required 3581 hours (about 21 weeks) on one of the fastest available PCs. The produced certificate is a text file containing nearly $5\,800\,000$ characters (please count how many books, more boring than this one, would be needed to contain them). Using the existing certificate, primality of the number can be verified within less than two days.

To illustrate the extraordinary progress that has been achieved in the performance of the ECPP method during the past years, here are the previous records:

Prime number	Digits	Date
$10^{5019} + (3^2 \times 7^5 \times 11^{11})$	5020	September 2001
$10^{3999} + 4771$	4000	May 2001
$(348^{1223} - 1)/347$	3106	January 2001
$(30^{1789} - 1)/29$	2642	October 2000
$(2^{7331} - 1)/458072843161$	2196	October 1997

Except for the last one, these records were due to the brothers G. and M. La Barbera and to Martin. The last prime, which is the second and largest factor of the Mersenne number

$$M_{7331} = 458072843161 \times P2196,$$

was verified by E. Mayer and F. Morain using Morain's ECPP program.

To feel how well a general purpose primality test performs, it is a good idea to apply the test to random numbers, namely, numbers whose digits were obtained by repeatedly spinning a wheel with ten possible positions. Some numbers which appear in nature, like the ubiquitous constant π, seem to have randomly distributed digits in their decimal part.

Indeed, in September 1999 more than 206 billion decimal digits of π were calculated by Y. Kanada and his coworkers. A statistical analysis confirms that any given succession of digits appears as often as it should be expected from randomness. In particular, Caldwell & Dubner (2000) analysed the occurrence of primes made out of a sequence of successive digits of π, obtaining a remarkable agreement.

More recently, in December 2002, Kanada announced that he had calculated 1.2411 trillion digits of π; for details, see Bailey (2003). This brings to a true story, not to be forgotten. Ludolph van Ceulen became famous for having calculated 35 correct digits of π (published posthumously in 1615). These digits were inscribed in his epitaph. I wish long life to Kanada—his epitaph will create problems.

Monte Carlo methods

Early in this century, the casino in Monte Carlo attracted the aristocracy and adventurers, who were addicted to gambling. Tragedy and fortune were determined by the spinning wheel.

I read with particular pleasure the novel by Luigi Pirandello, telling how the life of Mattia Pascal was changed when luck favored him, both at Monte Carlo and in his own Sicilian village. But Monte Carlo is not always so good. More often, total ruin, followed by suicide, is the price paid!

As you enter into the Monte Carlo primality game, and if your Monte Carlo testing will be unsuccessful, I sincerely hope that you will not be driven to suicide.

I wish to mention three Monte Carlo tests, due to Baillie & Wagstaff (1980), Solovay & Strassen (1977) and Rabin (1976, 1980). In each of these tests a number of witnesses a are used, in connection with congruences like those satisfied by $\mathrm{psp}(a)$, $\mathrm{epsp}(a)$, $\mathrm{spsp}(a)$ numbers.

I describe briefly Rabin's test, which is very similar to Miller's. Based on the same idea of Solovay & Strassen, Rabin proposed the following test:

Step 1. Choose, at random, $k > 1$ small numbers a, such that $1 < a < N$ and $\gcd(a, N) = 1$.

Step 2. Test, in succession, for each chosen basis a, whether N satisfies the condition in the definition of a strong pseudoprime in base a; writing $N - 1 = 2^s d$, with d odd, $s \geq 0$, either $a^d \equiv 1 \pmod{N}$ or $a^{2^r d} \equiv -1 \pmod{N}$ for some r, $0 \leq r < s$.

If an a is found for which the above condition does not hold, then declare N to be composite. In the other case, the probability that N is a prime, when certified prime, is at least $1 - 1/4^k$. So, for $k = 30$, the likely error is at most one in 10^{18} tests.

You may wish to sell prime numbers—yes, I say sell—to be used in public key cryptography (be patient, I will soon come to this application of primality and factorization). And you wish to be sure, or sure with only a negligible margin of error, that you are really selling a prime number, so that you may advertise: "Satisfaction guaranteed or money back."

On the basis of Rabin's test, you can safely develop a business and honestly back the product sold.

The recent AKS test

In August 2002, Agrawal, Kayal & Saxena posted in their website a paper containing an algorithm for primality testing which is for general purpose, deterministic, fully justified *and* runs in polynomial time. This solved the long-standing problem mentioned earlier in this subsection.

The theoretical basis of the test is a proposition which, except at one step, involves only arguments dealing with simple polynomials with coefficients in integers modulo N, and a binomial. The crucial step, presently required, is a deep theorem of Fouvry pertaining to

sieve theory. I like to state this theorem (not in the stronger original form):

Let $\theta = 0.6687\ldots > 2/3$. For every $x > 2$ there exists a prime p such that $x^\theta < p < x$, and there exists k, not a multiple of 3, such that $2kp + 1 \leq x$ and $2kp + 1$ is a prime.

It is reasonable to hope that the test will be suitably modified and perhaps become dependent on a less profound theorem than Fouvry's.

As for the running time (with fast multiplication), it was originally evaluated as essentially $(\log N)^{12}$, and lately lowered to $(\log N)^{7.5}$. An analysis of the running time may also be found in Morain's pre-print (2002).

I have asked Agrawal to prepare a short presentation of the AKS algorithm, which I reproduce here. I am thankful for his collaboration.

The central idea in the new primality testing algorithm is the following identity characterizing primes:

N is prime if and only if $(1 - X)^N \equiv 1 - X^N \pmod{N}$.

The simplest way of verifying this identity efficiently is to choose a random small degree polynomial $Q(X)$ and check the identity modulo $Q(X)$. With high probability the result will be correct. This gives a very simple randomized polynomial time algorithm.

To get a deterministic algorithm, one way is to show that if the identity is false, then modulo only a "few" small degree polynomials $Q(X)$ the check will fail. And one of the simplest sets of such polynomials is $Q(X) = X^r - 1$ for small degrees r.

In what follows, let $P_1(X) \equiv P_2(X) \pmod{X^r - 1, n}$ denote the identity of the remainders of $P_1(X)$ and $P_2(X)$ after division by $X^r - 1$ and after dividing the coefficients by n. Then the following weaker version of the above statement is proved:

$N = p^k$ (where p is a prime) if and only if $(a - X)^N \equiv a - X^N \pmod{X^r - 1, p}$ for a "few" values of a and r.

In fact, r can be fixed to be a specific value. The characterization immediately gives a deterministic and efficient primality test as the identity can be verified modulo N (but not modulo p, of course), and the standard method can be used to handle the case when N is a non-trivial power of p.

One direction of the equivalence is trivial to show. To prove the other direction use is made of the following facts:

(i) If $(a - X)^N \equiv a - X^N \pmod{X^r - 1, p}$ for several values of a, then for any polynomial $g(X)$ in the multiplicative group generated by the corresponding linear polynomials $(a - X)$, the following property holds:

$$g(X)^N \equiv g(X^N) \pmod{X^r - 1, p}.$$

This gives exponentially many polynomials $g(X)$ satisfying the identity, provided the order of p modulo r is large, and this can be ensured using existing results in sieve theory.

(ii) If $g(X)^N \equiv g(X^N) \pmod{X^r - 1, p}$, as above, and $g(X)^p \equiv g(X^p) \pmod{X^r - 1, p}$ (trivially), then for any $s = n^i p^j$,

$$g(X)^s \equiv g(X^s) \pmod{X^r - 1, p}.$$

(iii) Since powers of X are reduced modulo $X^r - 1$, there exist s and t, $s \neq t$, such that

$$g(X)^s \equiv g(X^t) \pmod{X^r - 1, p}.$$

This is not possible when both s and t are smaller than the size of the group in (i), but this is ensured, as noted above, by known results in sieve theory.

C   TITANIC AND CURIOUS PRIMES

In an article of 1983/84, Yates coined the expression "titanic prime" to name any prime with at least 1000 digits. In the paper with the suggestive title *Sinkers of the Titanics* (1984/85), Yates compiled a list of the largest known titanic primes. By January 1, 1985, he knew 581 titanic primes, of which 170 had more than 2000 digits. These were listed in the paper.

In September 1988, Yates' list comprised already 876 titanic primes. The *Six of Amdahl* (J. Brown, L.C. Noll, B. Parady, G. Smith, J. Smith & S. Zarantonello) announced at the beginning of 1990 the discovery of 550 new titanic primes.

It is not surprising that these primes have special forms, a few being Mersenne primes, others being of the form $k \times 2^n \pm 1$, or $k \times$

$b^n + 1$ $(b > 2)$. The reason is simply that there are more efficient primality testing algorithms for numbers of these forms.

In 1992, Yates called *gigantic* all primes with at least 10000 digits. For primes with $1\,000\,000$ or more digits, we use the expression *megaprimes*; as it was mentioned, the largest Mersenne primes are megaprimes. After Yates' death, C. Caldwell became the keeper of the titanic primes, gigantic primes, and other jewels. But he is also the author and manager of a very informative and up-to-date Internet site about "matters primes". I benefited from visiting this site—it is not less interesting than the San Diego Zoo.

The rapid progress of primality testing increased these lists, almost every day. At the end of 2002, the 5000 largest known primes (the only ones displayed in Caldwell's list) had more than 30000 digits. It would be futile to try to report these numbers. Since there are already more known titanic, gigantic and megaprimes than the total number of lines of this book, I do not have bad conscience with this omission. However, it would be unforgivable to hide the following curiosities from you.

A *palindromic* number (in base 10) is an integer $N = a_1 a_2 \ldots a_{n-1} a_n$ with decimal digits a_i $(0 \leq a_i \leq 9)$ such that $a_1 = a_n$, $a_2 = a_{n-1}$, $\ldots$. Due to the survival of the old mysticism attached so often to numbers (perfect numbers, amicable numbers, abundant numbers, etc.), the palindromic numbers still command the attention of numerologists.

For many years, Dubner has been finding larger and larger palindromic prime numbers, keeping safe his title of record man until 2001, when he found the prime $10^{39026} + 4538354 \times 10^{19510} + 1$, with 39027 digits.

Record

The largest known palindromic prime is $10^{104281} - 10^{52140} - 1$, a number with 104281 digits. It was found in January 2003 by D. Heuer using a program called PrimeForm, whose developers include C. Nash, Y. Gallot and G. Woltman.

An earlier record by Dubner, was a number that might be called a triply palindromic prime: $10^{35352} + 2049402 \times 10^{17673} + 1$; it has 35353 digits—a number which is again a palindromic prime, with 5 digits, and where 5 is again a palindomic prime!

We may consider the following, apparently silly problem: Given $k \geq 4$, to determine a sequence $N_1, N_2, \ldots, N_k$, where each N_i is a palindromic prime and N_{i+1} is the number of digits of N_i (for $i = 1, \ldots, k-1$).

For the description of the subsequent pearls, the following notation is useful: $(23)_4$, for example, means 23232323, and $(1)_{15}$ means that the digit 1 is repeated 15 times; and so on.

RECORDS

A.   The largest known prime, all of whose digits are prime numbers (2, 3, 5, 7), is

$$73232352323272325252 \times \frac{10^{3120} - 1}{10^{20} - 1} + 1$$
$$= (73232352323272325252)_{156} + 1.$$

It has 3120 digits and was discovered by Dubner in 1992.

B.   The largest known prime with all digits equal to 0 or 1 is $1(0)_{15397}1110111(0)_{15397}1$, with 30803 digits. It is also a palindrome and was discovered by Dubner in 1999.

C.   The largest known primes with initial digit d (of course, not divisible by 3), followed by n digits equal to 9, are:

d	n	Year
1	55347	2002
2	49314	2002
4	21456	2001
5	34936	2001
7	49808	2002
8	48051	2000

Most of these primes were discovered by E.J. Sorensen. Only the last one was found by Dubner. In each case Gallot's program was used.

D.   The largest known prime with all digits odd is the number $1(9)_{55347}$ listed in the previous topic.

E.   The largest known prime number with the largest number of digits equal to 0 is $105994 \times 10^{105994} + 1$ and was discovered by G. Löh and Y. Gallot in 2000.

F.   The most exotic curious prime is

$(1)_{1000}(2)_{1000}(3)_{1000}(4)_{1000}(5)_{1000}(6)_{1000}(7)_{1000}(8)_{1000}(9)_{1000}(0)_{6645}1.$

This prime has 15646 digits and was discovered, of course, by Dubner (in 2000).

G.   And last (but surely least): The smallest prime with 1000 digits is $10^{999} + 7$. Its primality was verified by P. Mihăilescu in 1998.

D   FACTORIZATION

The factorization of large integers is a hard problem: there is no known algorithm that runs in polynomial time. It is also an important problem, because it has found a notorious application to public key cryptography.

Nevertheless, I shall not discuss here the methods of factorization—this would once again lead me too far from the subject of records on prime numbers. The best I can do is to quote some books and research papers, which may serve as an Ariadne thread in the labyrinth. Recommended books are, in chronologocal order, the following.

The volume by Brillhart, Lehmer, Selfridge, Tuckerman & Wagstaff (1983) contains tables of known factors of $b^n \pm 1$ ($b = 2$, 3, 5, 6, 7, 10, 11, 12) for various ranges of n. For example, the table of factors of $2^n - 1$ extends for $n < 1200$; for larger bases b, the range is smaller. The second edition of the book, which appeared in 1988, contains 2045 new factorizations, reflecting the important progress accomplished in those few years, both in the methods and in the technology. The recent third edition includes another 2332 new factorizations.

This collective work, also dubbed "the Cunningham project", was originally undertaken to extend the tables published by Cunningham & Woodall in 1925. It is likely that this activity will go on unabated. Heaven is the limit!

The book of Riesel (1985) discusses factorization (and primality) at length. It also contains tables of factors of Fermat numbers, of Mersenne numbers, of numbers of the forms 2^n+1, 10^n+1, of repunits $(10^n-1)/9$, and many more. It is a good place to study techniques of factorization, which are exposed in a coherent and unified way. Due to its deserved success, a second updated edition has appeared in 1994, which also contains a description of the elliptic curve factoring method.

In 1989, Bressoud published an undergraduate text on factorization and primality. It contains not only the standard background, but also the quadratic sieve and elliptic curve methods.

Among the expository papers, the following deserve attention: Guy (1975) discusses the methods now considered classical; Williams (1984) covers about the same ground, being naturally more up to date—it is pleasant reading. Dixon (1984) writes about factorization as well as on primality. The lecture notes of a short course by Pomerance (1984) contain an annotated bibliography.

To quote more technical papers, the use of elliptic curves in factoring may be read, first hand, in the paper by Lenstra (1987); the paper of the brothers Lenstra of 1990 is also of fundamental importance. More recently, I indicate a paper on the number field sieve, by the brothers Lenstra, Manasse & Pollard (1993).

Just as an illustration, and for the delight of lovers of large numbers, I will give now explicit factorizations of some Mersenne, Fermat, and other numbers; for the older references, see Dickson's *History of the Theory of Numbers*, Vol. I, pp. 22, 29, 377, and Archibald (1935):

$$M_{59} = 2^{59} - 1 = 179951 \times 3203431780337,$$

by Landry in 1869;

$$M_{67} = 2^{67} - 1 = 193707721 \times 761838257287,$$

by Cole in 1903, already mentioned;

$$M_{73} = 2^{73} - 1 = 439 \times 2298041 \times 9361973132609,$$

the factor 439 by Euler, the other factors by Poulet in 1923;

$$F_6 = 2^{2^6} + 1 = (1071 \times 2^8 + 1) \times (262814145745 \times 2^8 + 1)$$
$$= 274177 \times 67280421310721,$$

by Clausen in 1856.

The above factorizations were obtained before the advent of computers!

More recently, the following factorizations were obtained:

$$M_{113} = 2^{113} - 1 = 3391 \times 23279 \times 65993 \times 1868569$$
$$\times 1066818132868207,$$

the smallest factor by Reuschle in 1856, and the remaining factors by Lehmer in 1947;

$$M_{193} = 2^{193} - 1 = 13821503 \times 61654440233248340616559$$
$$\times 14732265321145317331353282383,$$

by Naur (1983) and, independently, by Pomerance & Wagstaff in 1983. The next factorization has direct historical connection with Mersenne himself (see Section VII):

$$M_{257} = 2^{257} - 1 = 535006138814359$$
$$\times 1155685395246619182673033$$
$$\times 374550598501810936581776630096313181393,$$

by Penk and by Baillie, who found, respectively, the first and the two last factors in 1979, resp. 1980; note that already in 1927, Lehmer had shown that M_{257} is composite, without however finding any factor.

Turning to Fermat numbers, we have:

$$F_7 = 2^{2^7} + 1 = 59649589127497217 \times 5704689200685129054721,$$

by Morrison & Brillhart in 1970 (published in 1971);

$$F_8 = 2^{2^8} + 1 = 1238926361552897$$
$$\times 93461639715357977769163558199606896584051237541638188580280321,$$

by Brent & Pollard in 1980 (published in 1981).

The Fermat number F_{11} has been completely factored in 1988. Two small prime factors were long well-known; two more prime factors were found by Brent (with the elliptic curve method), who indicated that the 564-digit cofactor was probably a prime; this was shown to be the case by F. Morain.

The number F_9 was factored in 1990 by A.K. Lenstra and M.S. Manasse. It could not resist the number field sieve method. The most recently factored Fermat number is F_{10}; the factorization was completed by Brent in 1995.

All this, and much more, was said in the sections dealing with Fermat and Mersenne numbers.

In a paper of 1988, dedicated to Dov Jarden, Brillhart, Montgomery & Silverman gave the known factors of Fibonacci numbers U_n

(for n odd, $n \leq 999$) and of Lucas numbers V_n (for $n \leq 500$). The factorizations were complete to $n \leq 387$ and $n \leq 397$, respectively. In April 2003, Montgomery reported that the factorizations of U_n and V_n had been finished for all $n \leq 1000$. This pushes much further the work which had been done by many other numerologists, among whom Jarden (see the third edition of his book, 1958).

Here are some more noteworthy factorizations, which at their time represented an important step forward:

$$\frac{10^{103} + 1}{11} = 1237 \times 44092859 \times 102860539 \times 984385009$$
$$\times\ 612053256358933 \times 18272511148665211155647161$$
$$\times\ 1471865453993855302660887614137521979,$$

factorization completed by Atkin and Rickert in 1984.

A.K. Lenstra and M.S. Manasse were "pleased to announce a first factorization of a 100-digit number by a general purpose factorization algorithm" (October 12, 1988); such an algorithm factors a number N in a deterministic way, based solely on the size of N, and not on any particular property of its factors; in its worst case, the running time for factorization is nearly the same as the average running time.

The happy number was

$$\frac{11^{104} + 1}{11^8 + 1} = 86759222313428390812218077095850708048977$$
$$\times\ 108488104853637470612961399842972948409834611525790577216753.$$

The number field sieve method was used to completely factor the 138-digit number $2^{457} + 1$, which is equal to $3 \times P49 \times P89$, Pn denoting a prime with n digits. This was one of the good successes of the special number field sieve (SNFS) method, achieved by A.K. Lenstra and M.S. Manasse in November 1989; newspapers reported this feat, sometimes at front page!

In 1992, A.K. Lenstra and D. Bernstein factored the 158-digit Mersenne number M_{523} into two prime factors with 69 and 90 digits respectively, using an SNFS implementation on two massively parallel supercomputers.

An extraordinary factorization was announced in April 1999 by a group calling itself *The Cabal*. Using SNFS again, they factored the repunit number $(10^{211} - 1)/9$ into a product $P93 \times P118$, establishing

a record for the largest penultimate prime factor ever found. This was the collective effort of S. Cavallar, B. Dodson, A. Lenstra, P. Leyland, W. Lioen, P. Montgomery, H. te Riele and P. Zimmermann.

In the following subsection I shall discuss public key cryptography, where numbers are involved which should be extremely difficult to factorize.

For a deeper understanding of primality and factorization, I warmly recommend the new book by Crandall & Pomerance (2001). It contains the most important methods and proofs and was written by two renowned authorities in the subject.

Anyone interested in primality testing, factorization, or similar calculations with very large numbers needs, of course, access to high-speed sophisticated computers of the latest generation. There is still pioneering work to be done in the development of gadgets adaptable to personal computers. These will allow us to reach substantial results in the comfort of home. If it is snowing outside—as is often the case in Canada—you may test your prime, keeping warm feet.

E   Public Key Cryptography

Owing to the proliferation of means of communication and the need to send messages—like bank transfers, love letters, instructions for buying stocks, secret diplomatic information, as, for example, reports of spying activities—it has become very desirable to develop a safe method of coding messages. In the past, codes have been kept secret, known only to the parties sending and receiving the messages, but it has often been possible to study the intercepted messages and crack the code. In simpler cases, it would be enough to study the frequency of symbols in the message. In war situations, this had disastrous consequences.

Great progress in cryptography came with the advent of public key crypto-systems. The main characteristics of the system are its simplicity, the public key, and the extreme difficulty in cracking it. The idea was proposed in 1976 by Diffie & Hellman, and the effective implementation was proposed in 1978 by Rivest, Shamir, & Adleman. This crypto-system is therefore called the RSA-system. I shall describe it now.

Each letter or sign, including blank space, corresponds to a 3-digit number. In the *American Standard Code for Information Interchange* (ASCII), this correspondence is the following:

—	A	B	C	D	E	F	G	H
032	065	066	067	068	069	070	071	072

I	J	K	L	M	N	O	P	Q
073	074	075	076	077	078	079	080	081

R	S	T	U	V	W	X	Y	Z
082	083	084	085	086	087	088	089	090

Each letter or sign of the message is replaced by its corresponding 3-digit number, giving rise to a number M, which represents the message.

Each user A of the system lists in a public directory his key, which is a pair of positive integers: (n_A, s_A). The first integer n_A is a product of two primes, $n_A = p_A q_A$, which are chosen to be large and are kept secret. Moreover, s_A is chosen to be relatively prime with both $p_A - 1$, $q_A - 1$.

To send a message M to another user B, A encrypts M—the way to encode M depends on who will receive it. Upon receiving the encoded message from A, the user B decodes it using his own secret decoding method.

In detail, the process goes as follows. If the message $M \geq n_B$, it suffices to break M into smaller blocks; so it may be assumed that $M < n_B$. If $\gcd(M, n_B) \neq 1$, a dummy letter is added to the end of M, so that for the new message, $\gcd(M, n_B) = 1$.

A sends to B the encoded message $E_B(M) = M'$, $1 \leq M' < n_B$, where M' is the residue of M_{s_B} modulo n_B: $M' \equiv M^{s_B} \pmod{n_B}$.

In order to decode M', the user B calculates t_B, $1 \leq t_B < (p_B - 1)(q_B - 1) = \varphi(n_B)$, such that $t_B s_B \equiv 1 \pmod{\varphi(n_B)}$; this is done once and for all. Then

$$D_B(M') = M'^{t_B} \equiv M^{s_B t_B} \equiv M \pmod{n_B},$$

so B may read the message M. How simple!

In truth, as it always happens, some technical problems appear. They are discussed in specialized books and numerous articles. Here I adopt a simplistic point of view, illustrated with an example. To make it easier, the message is encoded by groups of two letters— which is not what happens in practice.

Now put your hand in your pocket and pick up your little calculator. Below is an encoded message which a certain person is sending to an individual whose public key is (n, s), where $n = 156287$, $s = 181$:

15147403692507697411796402929902665403692510174310970109517915207006804505517600832900157414996603153311786415459901390703153301398601235306804513375012651013734911786411333812898611786411005204760700157401073800377209664211786407083810914501109811786402860011786405654711786408356704127110914505600

You don't know the secret prime factors of n. Can you decode the message? The answer is printed somewhere in this book.

I shall now say a little bit on how to crack the crypto-system. It is necessary to discover $\varphi(n_A)$ for each user A. This is equivalent to the factorization of n_A. Indeed, if p_A, q_A are known, then $\varphi(n_A) = (p_A - 1)(q_A - 1)$. Conversely, putting $p = p_A$, $q = q_A$, $n = n_A$, from $\varphi(n) = (p - 1)(q - 1) = n + 1 - (p + q)$, $(p + q)^2 - 4n = (p - q)^2$ (if $p > q$), then

$$p + q = n + 1 - \varphi(n),$$
$$p - q = \sqrt{[n + 1 - \varphi(n)]^2 - 4n},$$

and from this, p, q are expressed in terms of n, $\varphi(n)$.

There is much more to be said about the RSA crypto-system:

(a) how to send "signed" messages, so that the receiver can unmistakably identify the sender;

(b) how to choose well the prime factors of the numbers n_A of the keys, so that the cracking of the system is unfeasible with currently known means.

In relation to (b), it is of foremost importance for the protection of the message that the public key can not be factorized. So, how many digits should the key have in order to make the potential factoring time prohibitive?

To test this point, various keys have been proposed to mathematicians as a factoring challenge. Among them was the following 512-bit number, called RSA-155 to indicate that it has 155 decimal digits:

RSA-155 =
109417386415705274218097073220403576120037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933543333897

This number had carefully been generated as a possible key for the Rivest-Shamir-Adleman method. The challenge to factorize it was broken in August 1999 by a team of scientists from six different countries, led by H. te Riele. They used the general number field sieve to disclose the following two 78-digit prime factors:

> 1026395928297411057720541965739916759007165678080380668034193352179071307779,
>
> 106603488380168454820927220360012878679207958575989291522270608237193062808643

This breakthrough showed, much earlier than expected when the practical use of the RSA method was started, that the popular key-size of 512 bits is no longer safe. As a result, 768-bit keys (about 230 digits) are now recommended as the minimum for achieving reliable security. Their two prime factors p, q, chosen at random, should be of equal size.

The current RSA factoring challenge includes, in a notation indicating number of bits, the numbers RSA-576 (174 decimal digits) through RSA-2048 (617 digits). Rewards range from \$10,000 to \$200,000 (US Dollars).

For all these questions, the reader may consult the original papers of Rivest, Shamir & Adleman (1978), and of Rivest (1978). There are, of course, many expository papers and books on the subject. See the paper by Couvreur & Quisquater (1982) as well as— pardon me the other writers of nice expository papers—the books of Riesel (1985), Koblitz (1987), Bressoud (1989), Coutinho (1999), and Wagstaff (2003). And, for example, the lecture notes of Lemos (1989), which are written in Portuguese—it is like studying cryptography in an encrypted language. Perhaps all this at Copacabana Beach.