PSEUDOPRIMES: A SURVEY OF RECENT RESULTS

François Morain * †

LIX, Laboratoire d'Informatique de l'Ecole Polytechnique Ecole Polytechnique, 91128 Palaiseau Cedex, France

1 Introduction

Public key cryptosystems require the use of large prime numbers, numbers with at least 256 bits (80 decimal digits), see for example [12]. One needs to generate these numbers as fast as possible. One way of dealing with this problem is the use of special primes built up using the converse of Fermat's theorem [35, 14, 17, 29]. Another is to use sophisticated primality proving algorithms, that are fast but need a careful implementation [13, 9].

In another direction, one can be happy with a number declared prime by a compositeness test, such as Miller-Rabin's. Numbers which pass this test, but are nevertheless composite, are called pseudoprimes. There are different species of pseudoprimes. This kind of compositeness algorithm requires a very good ratio between the programming work needed and the results achieved.

In this paper, we aim at presenting the most recent results achieved in the theory of pseudoprime numbers. First of all, we make a list of all pseudoprime varieties existing so far. This includes Lucas-pseudoprimes and the generalization to sequences generated by integer polynomials modulo N, elliptic pseudoprimes. We discuss the making of tables and the consequences on the design of very fast primality algorithms for small numbers. Then, we describe the recent work of Alford, Granville and Pomerance, in which they prove that there

*On leave from the French Department of Defense, Délégation Générale pour l'Armement.

†Research partially supported by the Programme de Recherches Coordonnées (PRC) Maths-Info.

exists an infinite number of Carmichael numbers. We also discuss the potential applications of their work to other classes of numbers.

2 All kinds of pseudoprimes

2.1 The ancestor

Let us start with the simplest kind of pseudoprimes. Fermat's little theorem tells us that if p is a prime number and a an integer prime to p, then

$$a^{p-1} \equiv 1 \bmod p. \tag{1}$$

A composite number p for which (1) holds is called a *pseudoprime to base a* (or psp-a for short). The smallest psp-2 is $N = 341 = 11 \times 31$.

It is known that for each value of a, there is an infinite number of psp-a (see [37]). A composite number p for which (1) holds for all values of a prime to p is called a *Carmichael number*. The smallest one is $561 = 3 \times 11 \times 17$. Until recently, it was not known that these numbers formed an infinite set (see section `xx`). Many properties of pseudoprimes are to be found in [37].

2.2 Refinements

A refined test is one due to Miller and Rabin [38]. Write $N - 1 = 2^t N_0$ with $2 \nmid N_0$. Then:

$$a^N - 1 = (a^{N_0} - 1)(a^{N_0} + 1) \times \cdots \times (a^{2^{t-1}N_0} + 1).$$

If N is prime, it divides the left hand side and thus must divide the right hand side, so one of the factors on the right. A composite N which satisfies $a^{N_0} \equiv 1 \bmod N$ or $a^{2^j N_0} \equiv -1 \bmod N$ for some $0 \leq j < t$ is called a *strong pseudo-prime to base a* (in short spsp-a). It is known that a composite N can be a spsp-a for at most $1/4$ of the bases [32]. Some improvements to the scheme have been given by Damgård and Landrock [15] and also Davenport [16], who countered an attack of Arnault on the pseudoprimality routine of Axiom (see [5] and also [6] for the same attack on the routine of Maple).

Recently, Atkin [8] has generalized the concept of strong pseudoprimes to that of q strong pseudoprimes, q being a small prime. Precisely, a composite integer N such that $N-1 = q^t N_0$, $q \nmid N_0$, is called a q-strong pseudoprime to base a ($\mathrm{spsp}_q(a)$), if

$$N \mid 1 + B + B^2 + \cdots + B^{q-1}$$

where $b \equiv a^{N_0} \bmod N \not\equiv 1$ and $B = b^{q^{i-1}}$ with i the least integer for which $b^{q^i} \equiv 1 \bmod N$.

2.3 Making tables

Carmichael numbers were tabulated by many authors [25, 24, 33]. The function $C(x)$ which counts the number of Carmichael numbers up to x is of interest and was also tabulated. In particular, $C(10^{12}) = 8241$, $C(10^{15}) = 105212$, $C(10^{16}) = 246683$. Pinch's tables are available via anonymous ftp.

Tables of pseudoprimes also exist. The most recent one contains all psp-2 up to 10^{12}: There are 101629 of them [34]. Using these tables, Schroeppel [40] checked that there are only 37 composite numbers less than 10^{11} which are spsp-a for a in $\{2,3,5\}$. Only one remains if we add $a = 7$ (namely 3215031751), and none if $a = 11$ is added next.

2.4 Generalizations

2.4.1 Linear recurrences

The concept of pseudoprimes was generalized with other relations like (1). For instance, one can look at sequences of numbers defined modulo N for a given integer N. Let $f(X)$ be a polynomial with integer coefficients:

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0.$$

Let p be a prime number and let β_i be the m roots of f in a suitable extension of $\mathrm{GF}(p)$. Define the sequence V_n as

$$V_n = \beta_1^n + \beta_2^n + \cdots + \beta_m^n \bmod p.$$

Denote by L the splitting field of $f(X) \bmod p$ and G its Galois group. For each σ in G, define

$$V_{\sigma,r} = \sum_{i=1}^{m} \sigma(\beta_i)\beta_i^r$$

for all $0 \leq r \leq m-1$. Such a collection $V(\sigma)$ is called an *admissible signature* for p. The value of a signature depends on the splitting of $f(X)$ modulo p. A pseudoprime for f is now a composite integer N which has an admissible signature $V(\sigma)$ for some σ (in a suitable context).

For example, let f be a polynomial of degree 2: $f(X) = X^2 + a_1X + a_0$. Let D be its discriminant and p a prime number not dividing D. Select $\sigma = 1$. Then, it is easy to see that

$$(V_p, V_{p+1}) = \begin{cases} (a_1, a_1^2 - 2a_0) & \text{if } (D/p) = 1 \\ (a_1, 2a_0) & \text{if } (D/p) = -1. \end{cases}$$

A less trivial example is the following [3]. Let $f(X) = X^3 - rX^2 + sX - 1$ where s and r are integers. Let α, β, γ be the roots of $f(X)$ and p be a prime number. Then

$$(V_{p-1}, V_p, V_{p+1}) = \begin{cases} (3, r, r^2 - 2s) & \text{if } f(X) \text{ has three roots } \bmod p \\ (B, r, C) & \text{if } f(X) \text{ has one root } \bmod p \\ (D, r, s) & \text{otherwise} \end{cases}$$

In case 2, let α be the root of $f(X) \bmod p$; then $B \equiv -r\alpha^2 + (r^2 - s)\alpha \bmod p$ and $C \equiv \alpha^2 + 2\alpha^{-1} \bmod p$. In case 3, let $\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$ and $D \equiv (rs - 3 - \delta)/2 \bmod p$ (note that all the quantities B, C, D are integers modulo p). The conditions on f correspond to a particular action of the Galois group of $f \bmod p$. In case 1, the splitting field of f is $\mathrm{GF}(p)$ and the Galois group acts on the roots as $\alpha^p = \alpha$, $\beta^p = \beta$, $\gamma^p = \gamma$. In case 2, the splitting field is $\mathrm{GF}(p^2)$ and we have $\alpha^p = \alpha$, $\beta^p = \gamma$, $\gamma^p = \beta$. The third case corresponds to the splitting field of f being $\mathrm{GF}(p^3)$ and the Galois action is (say): $\alpha^p = \beta$, $\beta^p = \gamma$, $\gamma^p = \alpha$.

This work has been done by Gurak [21] and generalizes the concept of Lucas pseudoprimes [10] (this corresponds to second-order recurrences) and the work of [3, 1, 26, 2, 7] for third-order recurrences.

2.4.2 Other generalizations

For completeness, let us add that some authors have studied the properties of elliptic pseudoprimes [18, 31, 11, 19].

Let p be a prime number greater than 3. An elliptic curve E over $\mathbf{Z}/p\mathbf{Z}$ is given by two integers a and b such that the quantity $-16(4a^3+27b^2)$ is non-zero modulo p. The set of points of E, denoted by $E(\mathbf{Z}/p\mathbf{Z})$ is the set of pairs (x, y) in $\mathbf{Z}/p\mathbf{Z}$ such that $y^2 \equiv x^3 + ax + b \bmod p$. An abelian law is usually defined on $E(\mathbf{Z}/p\mathbf{Z})$, which is known as the *tangent-and-chord* method. This law is ordinarily noted additively. For details on the law, we refer for example to [23]. Denote by m the number of points on E. Lagrange's theorem tells us that if P is a point on E, then $mP = O_E$. In some particular cases, it is easy to compute m. For instance, let $-D$ be the discriminant of an imaginary quadratic field with class number 1. (We know that $-D \in \{-4, -3, -7, -8, -11, -19, -43, -67, -163\}$.) Then if $(-D/p) = -1$, the associated curve E has cardinality $p + 1$.

We can define elliptic curves over a ring $\mathbf{Z}/N\mathbf{Z}$ for a composite N. Let $-D$ be as above and E an associated curve together with a point P on E. We say N is an elliptic pseudoprime if and only if $(-D/N) = -1$ and $(N + 1)P = O_E$. One way of building such a number N is to write it as $N = p_1 \ldots p_r$ and impose that $(-D/p_i) = -1$ and $p_i + 1 \mid N + 1$ for all i.

3 There exists an infinite number of Carmichael numbers

3.1 Background

Recall that $\varphi(N)$ is the cardinality of $(\mathbf{Z}/N\mathbf{Z})^\times$ for any integer N and that $\lambda(N)$ is the maximal order of an element of $(\mathbf{Z}/N\mathbf{Z})^\times$. If $N = \prod_{i=1}^r p_i^{\alpha_i}$ is the decomposition of N as a product of disctint primes, one has $\varphi(N) = \prod_i \varphi(p_i^{\alpha_i}) = \prod_i p_i^{\alpha_i - 1}(p_i - 1)$ and $\lambda(N) = \mathrm{lcm}(\lambda(p_i^{\alpha_i}))$; $\lambda(p_i^{\alpha_i}) = \varphi(p_i^{\alpha_i})$ for odd p_i or $\alpha_i \leq 2$ and $\lambda(2^e) = 2^{e-2}$ for $e \geq 3$.

One can show that a squarefree composite number N is a Carmichael number if and only if for all $p_i \mid N$, one has $p_i - 1 \mid N - 1$. Equivalently, N is a Carmichael number if and only if $\lambda(N) \mid N - 1$. For all this, we refer for instance to [39].

We define the number of divisors of N to be $\tau(N)$ and the number of *prime* divisors of N to be $\omega(N)$.

3.2 First ingredient

The basic idea is simple. First choose an integer Λ with a large number of divisors and let k be an integer prime to Λ. Build the set

$$S(k, \Lambda) = \{p \text{ prime}, p \nmid \Lambda, k \mid p - 1 \mid k\Lambda\}.$$

Suppose now that N is a squarefree product of elements of $S(k,\Lambda)$ such that $N \equiv 1 \bmod \Lambda$. Then N is a Carmichael number, since $N \equiv 1 \bmod k$ by construction, and for all p dividing N, one has:

$$p - 1 \mid k\Lambda \mid N - 1.$$

3.3 Second ingredient

Let $(G, \times)$ be a finite Abelian group. Denote by $|G|$ the cardinality of G and by m the maximal order of an element of G. One can prove the following [41, 42, 30].

Theorem 1. Let g_1, g_2, ..., g_n be elements of G. If $n > m(1 + \log(|G|/m))$, there exists indices i_1, i_2, ..., i_r such that $g_{i_1} \times g_{i_2} \times \cdots \times g_{i_r} = 1$. □

One now remarks that the set $S(k,\Lambda)$ is naturally isomorphic to a subgroup of $G = (\mathbf{Z}/\Lambda\mathbf{Z})^\times$ (the set of elements of $(\mathbf{Z}/k\Lambda\mathbf{Z})^\times$ which are congruent to 1 mod Λ is isomorphic to $(\mathbf{Z}/\Lambda\mathbf{Z})^\times$. The important point is that G does not depend on k, but on Λ.

3.4 Building large sets $S(k,\Lambda)$

The idea of the proof is now simple. One must build a set $S(k,\Lambda)$ so large that

$$|S(k,\Lambda)| > \lambda(\Lambda)(1 + \log(\varphi(\Lambda)/\lambda(\Lambda))).$$

If this is the case, we can use the preceding Theorem to show that necessarily, there exists a product of elements of $S(k,\Lambda)$ which is congruent to 1 modulo Λ and thus a Carmichael number.

Let us choose

$$\Lambda = \mathrm{lcm}(2, 3, \ldots, m)$$

for some integer m. By a standard result in number theory [22], one has $\Lambda \sim \exp(m)$ when m goes to infinity. Let

$$N = \prod_{\substack{p < m^2 \\ p-1 \mid \Lambda}} p$$

where p denote a prime number. It can be shown that the number of prime factors of N is greater than $c_1 m^2/\log m$ for a fixed constant $c_1 > 0$ and m large enough. It follows that the number of divisors of N satisfies

$$\tau(N) > 2^{c_1 m^2/\log m}.$$

We now remark that $\tau(N) \gg \lambda(N)$ since $\lambda(N) \mid \Lambda$. There is some hope to build $S(k,\Lambda)$ such that its cardinality is not too far from $\tau(N)$ and thus greater than $\lambda(N)$.

In [4], the authors are able to prove that there exists an integer k, prime to N such that

$$|S(k,\Lambda)| \geq \tau(N)^{c_2}$$

for some positive constant $c_2 > 0$. With this, we have

$$\varphi(N) < N < \prod_{p<m^2} p \sim \exp(m^2)$$

leading to

$$\lambda(N) \log \varphi(N) < \exp(2m) < 2^{c_1 c_2 m^2 / \log m} < \tau(N)^{c_2}$$

and thus the inequality of Theorem 1 applies and there is at least one Carmichael number built up with the elements of $S(k, \Lambda)$.

The final result of [4] is then

Theorem. The function $C(x)$ is larger than x^c for all sufficiently large x and for any positive constant $c < 5/12(1 - 1/2\sqrt{e}) = 0.290\ldots$. □

3.5 Remarks

As a consequence of this result, one has a better bound for $C(x)$. It is conjectured by Erdős that one should have

$$C(x) = x^{1-(1+o(1)) \log\log\log x / \log\log x}$$

for all sufficiently large x. The preceding result is still far from that.

The work of [4] can be extended to show that for all fixed a, there exist infinitely many squarefree composite n such that all prime factors p of n satisfy $p - a \mid n - 1$. The same is true for $p^2 - 1 \mid n$. However, this does not work for $p - a \mid n - b$ for any b other than 0 and 1, or for $p^2 + 1 \mid n - 1$. These cases are important for other pseudoprimality tests (see above). Also, for any finite set $\mathcal{S}$ of positive integers, there are infinitely many integers n which are spsp-a for all a in $\mathcal{S}$, as well as Carmichael numbers. The number of such numbers up to x is greater than $x^{c(\mathcal{S})}$ for some constant $c(\mathcal{S}) > 0$.

From a practical point of view, it is possible to devise fast algorithms for building Carmichael numbers with a large number of prime factors. For this and generalizations to all kind of elliptic pseudoprimes, we refer to [27, 28, 20, 43].

4 Conclusion

Despite the apparition of two powerful primality proving algorithms, pseudoprimes tests are still interesting. The theory of pseudoprimes has seen a renewed attention due to the result of Adlford, Granville and Pomerance. No doubt that further results will follow, enabling one to get a fast and compact primality testing algorithm by combining different pseudoprimality tests.

Acknowledgment. The author would like to thank Carl Pomerance for his sending the papers [4] as well as [36], and for many interesting discussions on his work.

References

[1] W. Adams. Splitting of quartic polynomials. *Math. Comp. 43*, 167 (July 1984), 329–343.

[2] W. Adams. Characterizing pseudoprimes for third order linear recurrences. *Math. Comp. 48*, 177 (Jan. 1987), 1–15.

[3] W. Adams and D. Shanks. Strong primality tests that are not sufficient. *Math. Comp. 39*, 159 (July 1982), 255–300.

[4] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. Preprint, July 13th 1992.

[5] F. Arnault. Le test de primalité de Rabin–Miller : un nombre composé qui le "passe". Report 61, Université de Poitiers – Département de Mathématiques, Nov. 1991.

[6] F. Arnault. Carmichaels fortement pseudo-premiers. Manuscript, 1992.

[7] S. Arno. A note on Perrin pseudoprimes. *Math. Comp. 56*, 193 (Jan. 1991), 371–376.

[8] A. O. L. Atkin. Probabilistic primality testing. In *Analysis of Algorithms Seminar I* (1992), P. Flajolet and P. Zimmermann, Eds., INRIA Research Report XXX. Summary by F. Morain.

[9] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. Research Report 1256, INRIA, Juin 1990. Submitted to *Math. Comp.*

[10] R. Baillie and S. S. Wagstaff, Jr. Lucas pseudoprimes. *Math. Comp. 35*, 152 (Oct. 1980), 1391–1417.

[11] R. Balasubramanian and M. R. Murty. Elliptic pseudoprimes, II. Submitted for publication.

[12] G. Brassard. *Modern Cryptology*, vol. 325 of *Lect. Notes in Computer Science*. Springer-Verlag, 1988.

[13] H. Cohen and A. K. Lenstra. Implementation of a new primality test. *Math. Comp. 48*, 177 (1987), 103–121.

[14] C. Couvreur and J. Quisquater. An introduction to fast generation of large prime numbers. *Philips J. Research 37* (1982), 231–264.

[15] I. Damgård and P. Landrock. Improved bounds for the Rabin primality test. In *Proc. 3rd IMA conference on Coding and Cryptography* (1991), M. Ganley, Ed., Oxford University Press.

[16] J. H. Davenport. Primality testing revisited. In *ISSAC '92* (New York, 1992), P. S. Wang, Ed., ACM Press, pp. 123–129. Proceedings, July 27–29, Berkeley.

[17] D. Gordon. Strong primes are easy to find. In *Advances in Cryptology* (1985), T. Beth, N. Cot, and I. Ingemarsson, Eds., vol. 209 of *Lect. Notes in Computer Science*, Springer-Verlag, pp. 216–223. Proceedings Eurocrypt '84, Paris (France), April 9–11, 1984.

[18] D. M. Gordon. On the number of elliptic pseudoprimes. *Math. Comp. 52*, 185 (Jan. 1989), 231–245.

[19] D. M. Gordon and C. Pomerance. The distribution of Lucas and elliptic pseudoprimes. *Math. Comp. 57*, 196 (Oct. 1991), 825–838.

[20] D. Guillaume and F. Morain. Building Carmichael numbers with a large number of prime factors and generalization to other numbers. Research Report 1741, INRIA, Aug. 1992.

[21] S. Gurak. Pseudoprimes for higher-order linear recurrence sequences. *Math. Comp. 55*, 192 (Oct. 1990), 783–813.

[22] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*, 5th ed. Clarendon Press, Oxford, 1985.

[23] D. Husemöller. *Elliptic curves*, vol. 111 of *Graduate Texts in Mathematics.* Springer, 1987.

[24] G. Jaeschke. The Carmichael numbers to 10^{12}. *Math. Comp. 55*, 191 (July 1990), 383–389.

[25] W. Keller. The Carmichael numbers to 10^{13}. *AMS Abstracts 9* (1988), 328–329. Abstract 88T-11-150.

[26] G. C. Kurtz, D. Shanks, and H. C. Williams. Fast primality tests for numbers less than $50 \cdot 10^9$. *Math. Comp. 46*, 174 (Apr. 1986), 691–701.

[27] G. Löh. Carmichael numbers with a large number of prime factors. *AMS Abstracts 9* (1988), 329. Abstract 88T-11-151.

[28] G. Löh and W. Niebuhr. Carmichael numbers with a large number of prime factors, II. *AMS Abstracts 10* (1989), 305. Abstract 89T-11-131.

[29] U. M. Maurer. Fast generation of secure RSA-products with almost maximal diversity. In *Advances in Cryptology* (1990), J.-J. Quisquater, Ed., vol. 434 of *Lect. Notes in Computer Science*, Springer-Verlag, pp. 636–647. Proc. Eurocrypt '89, Houthalen, April 10–13.

[30] R. Meshulam. An uncertainty inequality and zero subsums. *Discrete Mathematics 84* (1990), 197–200.

[31] I. Miyamoto and M. R. Murty. Elliptic pseudoprimes. *Math. Comp. 53*, 187 (July 1989), 415–430.

[32] L. Monier. Evaluation and comparison of two efficient probabilistic primality testing algorithms. *Theoretical Computer Science 12* (1980), 97–108.

[33] R. Pinch. The Carmichael numbers to 10^{16}. In preparation, 1992.

[34] R. Pinch. The pseudoprimes up to 10^{12}. In preparation, Sept. 1992.

[35] D. A. Plaisted. Fast verification, testing and generation of large primes. *Theoretical Computer Science 9* (1979), 1–16.

[36] C. Pomerance. Carmichael numbers. To appear in *Nieuw Arch. Wisk.*, 1992.

[37] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr. The pseudoprimes to 25.10^9. *Math. Comp. 35*, 151 (1980), 1003–1026.

[38] M. O. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput. 9*, 2 (1980), 273–280.

[39] P. Ribenboim. *The book of prime number records*, 2nd ed. Springer, 1989.

[40] R. Schroeppel. Richard Pinch's list of pseudoprimes. E-mail to the NMBRTHRY list, June 1992.

[41] P. van Emde Boas. A combinatorial problem on finite abelian groups, II. Tech. Rep. ZW–007, Math. Centrum Amsterdam Afd. Zuivere Wisk., 1969. 60 pp.

[42] P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite abelian groups, III. Tech. Rep. ZW–008, Math. Centrum Amsterdam Afd. Zuivere Wisk., 1969.

[43] M. Zhang. Searching for large Carmichael numbers. To appear in *Sichuan Daxue Xuebao*, Dec. 1991.