Pseudoprimes and Classical Primality Tests

Sebastian Pancratz

2 March 2009

1 Introduction

This brief introduction concerns various notions of pseudoprimes and their relation to classical composite tests, that is, algorithms which can prove numbers composite, but might not identify all composites as such and hence cannot prove numbers prime. In the talk I hope to also present one of the classical algorithms to prove a number n prime. In contrast to modern algorithms, these are often either not polynomial-time algorithms, heavily depend on known factorisations of numbers such as $n-1$ or are restricted to certain classes of candidates n.

One of the simplest composite tests is based on Fermat's Little Theorem, stating that for any prime p and any integer a coprime to p we have $a^{p-1} \equiv 1 \pmod{p}$. Hence we can prove an integer $n > 1$ composite by finding an integer b coprime to n with the property that $b^{n-1} \not\equiv 1 \pmod{n}$.

Definition 1. Let $n > 1$ be an odd integer and $b > 1$ with $(b, n) = 1$. We call n a *pseudo-prime* to base b if $b^{n-1} \equiv 1 \pmod{n}$, that is, if the pair n, b satisfies the conclusion of Fermat's Little Theorem.

Definition 2. If n is a positive odd composite integer which is a pseudo-prime to all bases b, we call n a Carmichael number.

Using this criterion, we can easily check that e.g. $561 = 3 \times 11 \times 17$ is a Carmichael number. It has been shown that there are infinitely many Carmichael numbers [1].

Definition 3. Let $n > 1$ be an odd integer and $b > 1$ with $(b, n) = 1$. We call n an *Euler pseudo-prime* if $b^{(n-1)/2} \equiv (b|n) \pmod{n}$, that is, if the pair n, b satisfies Euler's criterion for the evaluation of Legendre symbols.

It is a fact, discovered independently by Solovay and Strassen as well as by Lehmer, that if $n > 1$ is an Euler pseudo-prime for all bases b then n is a prime number. Also, Solovay and Strassen [9] showed that for a given composite integer n, n is an Euler pseudo-prime for at most half of the bases $b \in \{1, \dots, n-1\}$. This result provides a fast probabilistic primality test.

Theorem 4. Let $n \geq 3$ be odd. Then n is prime iff $E(n) = (\mathbb{Z}/n\mathbb{Z})^*$ where $E(n) \subset (\mathbb{Z}/n\mathbb{Z})^*$ is the set of bases to which n is an Euler pseudo-prime.

Proof. For the interesting direction, suppose that $E(n) = (\mathbb{Z}/n\mathbb{Z})^*$ but n is composite. Then $b^{n-1} \equiv (b|n)^2 \equiv 1 \pmod{n}$ for all $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Thus n is a Carmichael number and hence square-free, so we can write $n = pr$ with p prime and $(p, r) = 1$. Choose a quadratic nonresidue g modulo p and choose an integer a such that $a \equiv g \pmod{p}$ and $a \equiv 1 \pmod{r}$. Using the rules to evaluate Jacobi symbols,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{pr}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{r}\right) = \left(\frac{g}{p}\right)\left(\frac{1}{r}\right) = (-1)(+1) = -1.$$

But by assumption $(a|n) \equiv a^{(n-1)/2} \pmod{n}$ and so $a^{(n-1)/2} \equiv -1 \pmod{r}$, contradicting $a \equiv 1$ $\pmod{r}$. □

Definition 5. Let $n > 1$ be an odd integer, write $n - 1 = 2^s t$ and let $b > 1$ be an integer with $(b, n) = 1$. We call n a *strong pseudo-prime* if either

(i) $b^t \equiv 1 \pmod{n}$, or

(ii) there exists an $r \in \{0, \dots, s-1\}$ such that $b^{2^r t} \equiv -1 \pmod{n}$.

It is not difficult (but slightly technical) to show that if n is a strong pseudo-prime to base b then n is also a an Euler pseudo-prime to base b. It is easy to prove that if p is an odd prime then p is a strong pseudo-prime to every base. As a partial converse, Knuth [4] showed that, for odd composite $n > 1$, n is a strong pseudo-prime to at most $n/4$ of the bases $b \in \{1, \dots, n-1\}$. The probabilistic primality test derived from this is called the *Rabin–Miller test* and it supersedes the Solovay–Strassen test in every way. Assuming the Generalised Riemann Hypothesis, it can be turned into a deterministic test using the following result[1].

Theorem 6. Let $n > 1$ a an odd composite integer. Assuming the Generalised Riemann Hypothesis, there exists an integer b coprime to n with $1 < b < 2(\log n)^2$ such that n is not a strong pseudo-prime to base b.

To shed some more light of how the Generalised Riemann Hypothesis is involved, without further proof we state a theorem of Ankeny, which can be found e.g. in [2]. First define

$$G(n) = \min\{x \in \mathbb{N} : (\mathbb{Z}/n\mathbb{Z})^* \text{ is generated by primes } \leq x\}.$$

Theorem 7 (Ankeny)**.** Assume the Generalised Riemann Hypothesis. Then $G(n)$ is $\mathcal{O}((\log n)^2)$. In particular, every non-trivial subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ omits a positve number that is $\mathcal{O}((\log n)^2)$.

2 Problems

Problem 1. Given $b > 1$, there exists infinitely many composite integers n such that n is a pseudo-prime to base b.

Problem 2 (Korselt, 1899)**.** A compositive integer $n > 1$ is a Carmichael number iff n is square-free and all prime factors p of n satisfy $p - 1 \mid n - 1$.

Problem 3. Show that if, for $k \geq 1$, the numbers $6k + 1$, $12k + 1$ and $18k + 1$ are all prime then their product is a Carmichael number.

Problem 4 (Erdős)**.** Let $p > 3$ be a prime number. Show that $(2^{2p} - 1)/3$ is a pseudo-prime to base 2.

Problem 5 (Rotkiewicz)**.** Let $p > 5$ be a prime number. Show that $(2^{2p} + 1)/5$ is a pseudo-prime to base 2.

Problem 6 (Malo; Sierpiński)**.** Let n be a pseudo-prime to base 2. Show that $2^n - 1$ is also a pseudo-prime to the base 2.

Problem 7. Let p be an odd prime. Then p is a strong pseudo-prime to every base b.

I have first found these problems in the Part II course *Number Theory* at the University of Cambridge by Prof. J.H. Coates in 2006–07, or in the books by Cohen [3] and Bach and Shallit [2]. At the moment, I do not know how to solve Problems 4, 5 and 6, although admittedly I have not spent much time on them. Supposedly, the last two of these problems are solved in [7], [5] and [8].

[1] I think the result is strongly related to this article by Miller [6], although the language there is slightly different.

References

[1] W.R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722.

[2] E. Bach and J. Shallit, *Algorithmic number theory, vol. 1: Efficient algorithms (foundations of computing)*, The MIT Press, 1996.

[3] H. Cohen, *A course in computational algebraic number theory*, Springer, 1993.

[4] D.E. Knuth, *The art of computer programming, vol. 2: Seminumerical algorithms*, Addison–Wesley, 1981.

[5] E. Malo, *Nombres qui, sans être premiers, vérifient exceptionellement une congruence de Fermat*, L'Intermédiaire Math. **10** (1903), 88.

[6] G.L. Miller, *Riemann's hypothesis and tests for primality*, STOC '75: Proceedings of seventh annual ACM symposium on Theory of computing (New York, NY, USA), ACM, 1975, pp. 234–239.

[7] A. Rotkiewicz, *Sur les formules donnant des nombres pseudopremiers*, Colloq. Math. **12** (1964), 69–72.

[8] W. Sierpiński, *Remarque sur une hypothèse des Chinois convernant les nombres* $(2^n - 2)/n$, Colloq. Math. **1** (1947), 9.

[9] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), no. 1, 84–85.