

Number Theory: Problem sheet 4

Solutions must be submitted by Thursday 12 May 2005

0. Download the notes on ‘Algorithms’ from the course website.
1. In each case, apply the Miller-Rabin test with the given base a to investigate the primality of the given number n . (Use the binary powering algorithm to find a^m modulo n for the appropriate numbers m , and show your working.)
 - (i) $n = 1105$, $a = 2$;
 - (ii) $n = 1729$, $a = 3$. [12]
2. In the Miller-Rabin algorithm, if n is a pseudoprime to base a , but not a strong pseudoprime to base a then a number b is found with $b \not\equiv \pm 1 \pmod{n}$ but with $b^2 \equiv 1 \pmod{n}$. Then $g = \gcd(b-1, n)$ is a nontrivial factor of n (see Q.9 of sheet 3). Explain how to modify the program given in the handout to find such a g if this case. Apply this method to factorize $n = 45979947301$ which is a pseudoprime (but not a strong pseudoprime) to base 2. [10]
3. Apply Pollard’s $p-1$ algorithm, showing your working, with base $a = 2$ to find a factor of n in the following cases:
 - (i) $n = 1849$;
 - (ii) $n = 5917$. [12]
4. Apply Pollard’s Rho algorithm, by hand, with given iteration function f and given initial value x_0 to find a nontrivial factor of n in the following cases:
 - (i) $n = 1363$, $f(x) = x^2 + 2$, $x_0 = 1$;
 - (ii) $n = 3959$, $f(x) = x^2 + 1$, $x_0 = 1$.In each case give the number of iterations needed. [12]
5. Using the MAPLE implementation of Pollard Rho from the website, find nontrivial factors of each of the following numbers n , using seed 1 and iteration function $f(x) = x^2 + 1$.
 - (i) $2^{47} - 1$;
 - (ii) $2^{71} - 1$;
 - (iii) $10^{24} - 3$.

In each case, give the number of iterations needed. (You should modify the given program to output the number k as well as g .) [15]

6. An early triumph of the Pollard Rho method was the factorization of $2^{256} + 1$, already known to be composite, by Brent and Pollard in 1980. They wrote up their proof in the paper ‘Factorization of the eighth Fermat number’, which was published in 1981 in the journal *Mathematics of Computation*, volume 36, pages 627–630.

Download this paper from the JSTOR archive: <http://uk.jstor.org/> (you need to be on campus to do this). Which iteration function did they use to factorize $2^{256} + 1$? What seed did they use? How long did their calculation take? What is their mnemonic for the factor? [9]

(If you are feeling energetic, repeat their calculation in MAPLE.)

7. Let p be a prime, and let q be a prime factor of $2^p - 1$. Prove that 2 has order p modulo q , and deduce that $q \equiv 1 \pmod{p}$.

Hence show that $2^{13} - 1$ and $2^{17} - 1$ are both prime, and find prime factors of each of $2^{23} - 1$ and $2^{29} - 1$.

More generally, again let p be prime, and let a be a positive integer with $p \nmid (a - 1)$. Let $m = (a^p - 1)/(a - 1)$, which is an integer, and let q be a prime factor of m . Prove first that $p \nmid m$ and so that $q \neq p$. Then prove that a has order p modulo q , and deduce that $q \equiv 1 \pmod{p}$.

By choosing $a = n!$, or otherwise, deduce that there are infinitely many primes q satisfying $q \equiv 1 \pmod{p}$. [30]

8. (Challenge problem) Let $F_n = 2^{2^n} + 1$. Show that F_n is prime if and only if there is a number a with $a^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$.