

MAT 311: Number Theory

Spring 2008

Solutions to HW6

- (a) Show that $m = 1111$ is composite using Fermat's Theorem.
(b) Do the same for $m = 1111111111$.
Since we are allowed to use calculators, it is easy: `pari` says $2^{1110} \equiv 1024 \pmod{1111}$, and $2^{11111111110} \equiv 1496324899 \pmod{1111111111}$. If those numbers were prime we would get 1. So they must be composite. \square
- Show that 2047 is composite by applying the strong pseudoprime test.
 $2047 - 1 = 2046 = 2 \cdot 1023$. For $a = 2$, we get $2^{1023} \equiv 1 \pmod{2047}$. For $a = 3$, we get $3^{1023} \equiv 1565 \pmod{2047}$ and $3^{2046} \equiv 1013 \pmod{2047}$. So 2047 is composite. \square
- Show that if m is a pseudoprime but not strongly pseudoprime, then the strong pseudoprime test together with Euclidean Algorithm provides an efficient means of locating a proper divisor of m .
- Use Pollard's ρ -method to locate proper divisors of 8131, 10277 and 199934971.
I'll do the problem only for 8131. The other two can be done similarly.
Pick $u_0 = 3$. Using the recursion $u_{i+1} \equiv u_i^2 + 1 \pmod{m}$, we get $u_i \equiv 10, 101, 2071, 4005, 5694, 3340$ for $i = 1, \dots, 6$. Since we see that $(u_6 - u_3, m) = (1269, 8131) = 47$, we stop: 47 is a proper divisor of 8131. \square
- Show that if $(a, m) = 1$ and m has a prime factor p such that $p - 1 \mid Q$, then $(a^Q - 1, m) > 1$.
If $p - 1 \mid Q$, then $a^Q \equiv 1 \pmod{p}$ by Fermat. So $a^Q - 1 = kp$ for some k . Thus, $(a^Q - 1, m) = (kp, m) > 1$ since $p \mid m$. \square