

HOMEWORK 4
Math 104 - Dr. Evans
UCSD Winter 2004
Due Thursday, January 29, 5:00PM

1. (a) Use Euclidean algorithm to find integers x and y such that $101x + 191y = 1$.
(b) Use the solution from part (a) to find an inverse of 101 modulo 191. Make your answer between 0 and 190.
2. Prove that for any two positive integers a and m , a has an inverse modulo m if and only if $\gcd(a, m) = 1$.
3. A quadratic residue for an odd prime p is a number b between 1 and $p - 1$ such that $x^2 \equiv b \pmod{p}$ has a solution. Find the quadratic residues for $p = 19$ and $p = 23$. In general, how many quadratic residues do you think there are for any odd prime p ?
4. Given that the prime p satisfies $3p = a^2 + 5b^2$ for some integers a and b , find explicit integers A and B (in terms of a and b) such that $2p = A^2 + 5B^2$.
Hint: The product of $a + b\sqrt{-5}$ times its complex conjugate equals $3p$. What would such a product become if one were to replace $a + b\sqrt{-5}$ by $(a + b\sqrt{-5}) \cdot \left(\frac{1+E\sqrt{-5}}{3}\right)$ where E is 1 or -1? You'll have to justify why the numbers you find are actually integers.
5. (a) If $p = a^2 + 5b^2$, prove that $p \equiv 1$ or $9 \pmod{20}$.
(b) If $2p = a^2 + 5b^2$, prove that $p \equiv 3$ or $7 \pmod{20}$.