Name ________________________ Math 332 Prelim 1
October 15, 2001 Instructor: Lawren Smithline

Solve the following problems. Justify your answers. Closed calculators, closed notes, closed book. Please state clearly any theorem you cite from class or the book. (You don't need to prove them again here.) All problems have equal weight. **55 minutes**.

1. a. Let $d = (28, 20)$. Compute d and find integers x, y such that $28x + 20y = d$.

b. Prove or disprove: For integers m, n, if $(m, n) = 1$, then $(m + n, mn) = 1$.

2. a. Find the (least positive integer) multiplicative inverse of 3 modulo 13.

2.b. What is the remainder of 3^{31} when divided by 31?

3. a. Decide whether each of the following is a Gauss prime: $3 + 0i$, $5 + 0i$, $91 + 0i$.
(The Gauss integers are the ring $\mathbf{Z}[i] = \{a + bi : a, b \in \mathbf{Z}, i^2 = -1\}$.)

b. How many congruence classes solve $x^2 - 4 \equiv 0$ (modulo 99)? What are they?

Solutions

1. a. Observe $28 = 4 \cdot 7$ and $20 = 4 \cdot 5$. So $d = 4$. A solution to $28x + 20y = 4$ is also a solution to $7x + 5y = 1$, and vice versa. There will be solutions with $|x| < 5$ and $|y| < 7$. By inspection, $x = 2, y = -3$ works.

1. b. This is a homework problem from assignment 1. If $(m, n) = 1$, then $(m, m + n) = 1$. If $(m, n) = 1$, then $(m + n, n) = 1$. If $(X, m) = 1$ and $(X, n) = 1$, then $(X, mn) = 1$. So, given $(m, n) = 1$, and substituting $X = m + n$, we see that $(m + n, mn) = 1$.

2. a. Solve $3x + 13k = 1$ for x. We can try the 12 possibilities 1 through 12. Solution: $x = 9$ is the inverse of 3.

2. b. By a theorem, for any prime p, $a^p \equiv a$ (modulo p). This is an immediate consequence of Fermat's little theorem. 31 is prime, so the answer is 3.

3. a. By a theorem in the book, the Gauss primes are: $a + bi$ such that $a^2 + b^2$ is an ordinary integer prime, and ordinary integer primes p such that $p \equiv 3$ (modulo 4). So 3 is a Gauss prime, $5 = (2 + i)(2 - i)$ is not, and $91 = 7 \cdot 13$ is not.

3. b. The prime power factors of 99 are 9 and 11. By the Chinese Remainder Theorem, a solution to $x^2 - 4 \equiv 0$ (modulo 99) corresponds exactly to a choice of solution for each of $x^2 - 4 \equiv 0$ (modulo 9) and $x^2 - 4 \equiv 0$ (modulo 11).

By inspection, there are two solutions to each and two times two is four, so there are 4 solutions to the original equation.

Two solutions are the congruence classes of 2 and -2. The other ones are A such that $A \equiv 2$ (modulo 9) and $A \equiv -2$ (modulo 11) and $-A$. $A = 2 + 2 \cdot 9 = 20$ works. So the other two solutions are 20 and -20.

Note: $97 \equiv -2$ and $79 \equiv -20$.