Math 42-Number Theory
Problem Set #7
Due Thursday, April 7, 2011

1. Factor 30 in $\mathbb{Z}[i]$. Is there an element of $\mathbb{Z}[i]$ with norm 30?

2. Factor 65 in $\mathbb{Z}[i]$. Is there an element of $\mathbb{Z}[i]$ with norm 65?

3. How many ways can 30 and 65 be written as a sum of two squares?

4. Use the Euclidean algorithm to find the GCD of $1+13i$ and $7-i$ in $\mathbb{Z}[i]$.

5. Find a solution (X, Y), where X and Y are in $\mathbb{Z}[i]$ to the equation $(7-i)X + (1+13i)Y = 5$.

6. Compute $2^{(p-1)/2} \mod p$ for $p = 3, 5, 7, 11, 13, 17$. For which of these primes is $\left(\frac{2}{p}\right) = 1$?

7. Consider the congruence mod 19:

$$(2)(4)(6)(8)(10)(12)(14)(16)(18) \equiv (2)(4)(6)(8)(-9)(-7)(-5)(-3)(-1) \mod 19$$

Factor out a 2 from each factor on the left side, and cancel what you can. What does this say about $\left(\frac{2}{19}\right)$?

8. Do the analogous computation from problem 7 for $p = 23$ to compute $\left(\frac{2}{23}\right)$.

9. Consider the congruence mod 11:

$$(3)(6)(9)(12)(15) \equiv (3)(-5)(-2)(1)(4) \mod 11$$

Factor out a 3 from each factor on the left side, and cancel what you can. What does this say about $\left(\frac{3}{11}\right)$?

10. Prove that given natural numbers a and b, there exist integers q, r, ε such that $a = bq + \varepsilon r$ where $\varepsilon = \pm 1$ and $0 \le r \le \frac{b}{2}$. Prove in addition, that $\varepsilon = (-1)^{\lfloor \frac{2a}{b} \rfloor}$. Here, $\lfloor x \rfloor$ means the greatest integer less than or equal to x, so for example $\lfloor \frac{1}{2} \rfloor = 0$, $\lfloor 2 \rfloor = 2$ and $\lfloor \pi \rfloor = 3$. You may assume that given a and b, there are integers q' and r' such that $a = bq' + r'$ and $0 \le r' < b$.

11. Extra Credit: Prove that there are infinitely many primes of the form $4k+1$. (Hint: Show that for any $N > 1$, there is a prime $p > N$ with $p \equiv 1 \mod 4$. Do this by setting $m = (N!)^2 + 1$ and considering the smallest prime p dividing m. Is $p > N$? Why must p be 1 mod 4?)