M3P14 EXAMPLE SHEET 3 SOLUTIONS

1. Give the prime factorizations, in $\mathbb{Z}[i]$, of the following elements of $\mathbb{Z}[i]$. Be sure to justify that each of the factors is prime!

1a. 51

We have $51 = 3 \cdot (4+i) \cdot (4-i)$; $4+i$ and $4-i$ are prime because their norm is prime; 3 is prime because all integers congruent to 3 mod 4 remain prime in $\mathbb{Z}[i]$.

1b. $8+i$

Note that $N(8+i) = 65$, so the primes dividing $8+i$ divide 65, and hence divide either 5 or 13. But $5 = (2+i)(2-i)$, and $13 = (2+3i)(2-3i)$. We have

$$\frac{8+i}{2-i} = \frac{(8+i)(2+i)}{5} = 3+2i.$$

So $8+i = (3+2i)(2+i)$. Both factors are prime because their norms are prime.

1c. $5+7i$

We have $N(5+7i) = 74$, so the primes dividing $5+7i$ divide either 2 or 37. We have $2 = (1+i)(1-i)$ and $37 = (6+i)(6-i)$. Now

$$\frac{5+7i}{1+i} = \frac{(5+7i)(1-i)}{2} = 6+i,$$

so $(5+7i) = (1+i)(6+i)$. Both factors are prime because their norms are prime.

2. Find a greatest common divisor, in $\mathbb{Z}[i]$, of the following elements of $\mathbb{Z}[i]$:

2a. 51 and $20+5i$

One can do this via the Euclidean algorithm, but it is easier here to simply factor both numbers. We have seen (1a) that $51 = 3(4+i)(4-i)$, and 3 does not divide $20+5i$, so we must check which of $(4+i)$ and $(4-i)$ divide $20+5i$. Dividing, we see that $(4+i)$ does and $4-i$ does not, so $4+i$ is a GCD of 51 and $20+5i$.

2b. 95 and $8+i$

We have $8+i = (3+2i)(2+i)$, so we must check which of these divides 95. It is clear that $(2+i)$ does, since $2+i$ divides 5 and hence 95. On the other hand $3+2i$ does not, as its norm is 13 which is relatively prime to 95. Thus the GCD is $2+i$.

3a. Let n be an integer. Show that if $4n$ is the sum of three squares, then so is n. [HINT: if $4n = a^2+b^2+c^2$, show that all of a, b, and c must be even.]

Reduce mod 4; we have $a^2+b^2+c^2 \equiv 0 \pmod 4$. Since any square mod 4 is zero or 1, the only possibility is that a^2, b^2, c^2 are zero mod 4. Then a, b, c are even; let $A = \frac{a}{2}$, $B = \frac{B}{2}$, $c = \frac{c}{2}$. Then $A^2 + B^2 + C^2 = \frac{a^2+b^2+c^2}{4} = n$.

3b. Show that if n has the form $4^t(8k + 7)$ for some nonnegative integer t and integer k, then n cannot be written as the sum of three squares. (In fact, these are the *only* numbers that cannot be written as the sum of three squares, but this is much harder.)

Using $3a$ repeatedly, it suffices to show that no number of the form $8k+7$ can be written as the sum of three squares. Reducing mod 8, we see that the squares mod 8 are $0, 1$, and 4. Thus for any a, b, c, each of a^2, b^2, c^2 is congruent to $0, 1$, or 4 mod 8. Let n be the number congruent to 1 mod 8 and m be the number congruent to 4 mod 8. The possibilities are:

- $n = m = 0$, $a^2 + b^2 + c^2$ is zero mod 8.
- $n = 0$, $m = 1$, $a^2 + b^2 + c^2$ is 4 mod 8.
- $n = 1$, $m = 0$, $a^2 + b^2 + c^2$ is 1 mod 8.
- $n = 1$, $m = 1$, $a^2 + b^2 + c^2$ is 5 mod 8.
- $n = 1$, $m = 2$, $a^2 + b^2 + c^2$ is 1 mod 8.
- $n = 2$, $m = 0$, $a^2 + b^2 + c^2$ is 2 mod 8.
- $n = 2$, $m = 1$, $a^2 + b^2 + c^2$ is 6 mod 8.
- $n = 3$, $m = 0$, $a^2 + b^2 + c^2$ is 3 mod 8.

Since $a^2 + b^2 + c^2$ is never 7 mod 8 the claim follows.

4. Prove Wilson's theorem: If p is prime, then $(p-1)! \equiv -1 \pmod p$. [Hint: when multiplying together all the nonzero congruence classes mod p, almost every class cancels with its inverse. Which ones don't?]

By definition, $(p-1)!$ is the product of the positive integers less than p. For each $a \in \mathbb{Z}$ with $1 \le a \le (p-1)$, there is a unique multiplicative inverse of a mod p, and thus a unique a' with $1 \le a' \le (p-1)$ and $aa' \equiv 1 \pmod p$. Note that $(a')' = a$.

Moreover, if $a' = a$, then $a^2 \equiv 1 \pmod p$, so $a \equiv \pm 1 \bmod p$. Thus if a is between 1 and $p-1$ and $a' = a$, then a is 1 or $(p-1)$.

Now we can pair each integer a between 2 and $p-2$ with the integer a'; this breaks the integers between 2 and $p-2$ into pairs whose product is 1 mod p. Thus the product of the integers between 2 and $p-2$ is 1 mod p; i.e. $(p-2)! \equiv 1 \pmod p$.

Then $(p-1)! = (p-1)(p-2)! \equiv p-1 \equiv -1 \pmod p$.

5. Use Fermat descent, starting with $557^2 + 55^2 = 26 \cdot 12049$ to write the prime 12049 as the sum of two squares.

Let $a_0 = 557$, $b_0 = 55$, $r_0 = 26$. In Fermat descent, given a_i, b_i, r_i with $a_i^2 + b_i^2 = r_i 12049$, we choose u_i, v_i congruent to a_i, b_i modulo r_i, and between $-\frac{r_i}{2}$ and $\frac{r_i}{2}$, and set:

$$a_{i+1} = \frac{a_i u_i + b_i v_i}{r_i}$$

$$b_{i+1} = \frac{a_i v_i - b_i u_i}{r_i}.$$

Then $a_{i+1}^2 + b_{i+1}^2 = r_{i+1}12049$ for some integer r_{i+1} less than r_i.

In this case we have:

$$u_0 = 11, v_0 = 3$$
$$a_1 = 242, b_1 = 41$$
$$a_1^2 + b_1^2 = 5 \cdot 12049$$
$$r_1 = 5$$
$$u_1 = 2, v_i = 1$$
$$a_2 = 105, b_2 = 32$$
$$a_2^2 + b_2^2 = 12049$$

6. For each of the following n, either write n as the sum of two squares, or prove that it is not possible to do so: 1865, 77077, 609, and 7501.

We have $1865 = 373 \cdot 5$. Both these factors are prime, congruent to 1 mod 4, so 1865 is the sum of two squares. We have $5 = (2^2 + 1^2) = (2 + i)(2 - i)$. We also have $373 = 18^2 + 7^2 = (18 + 7i)(18 - 7i)$. Thus $1865 - (2 + i)(18 + 7i)(2 - i)(18 - 7i) = (29 + 32i)(29 - 32i) = 29^2 + 32^2$.

We have $77077 = 7^2 \cdot 11^2 \cdot 13$. We have $13 = 2^2 + 3^2$, so $77077 = (77 \cdot 2)^2 + (77 \cdot 3)^2$.

We have $609 = 203 \cdot 3$; since 203 is not divisible by 3, 3 divides 609 exactly once. Since 3 is not a sum of squares, 609 cannot be either.

We have $7501 = 13 \cdot 577$. Now $13 = (2+3i)(2-3i)$, and $577 = 24^2 + 1^2 = (24+i)(24-i)$. Thus $7501 = (2+3i)(24+i)(2-3i)(24-i) = (45+74i)(45-74i)$, so $7501 = 45^2 + 74^2$.

For the solutions to problem 7, see the course notes; all of problem 7 was done in lecture.