Week 8 Summary

Lecture 15

Example: Given that $81 = \sqrt{-1}$ in $\mathbb{Z}_{193}$, use Fermat's method of descent to write 193 as a sum of two squares.
We are told that $81^2 + 1$ is divisible by 193, and calculating it we find that

$$81^2 + 1 = 34 \times 193.$$

Since $81 \equiv 13 \pmod{34}$ it follows that $13^2 + 1$ is a multiple of 34, and calculating it we find that

$$13^2 + 1 = 34 \times 5.$$

So $(81^2 + 1^2)(13^2 + 1^2) = 34^2 \times 5 \times 193$. Now use either

$$\begin{aligned} &(a^2 + b^2)(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2 \\ \text{or} \qquad &(a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2 \end{aligned}$$

choosing whichever expression permits the cancellation of the squared factor (which is 34^2 in this example). Since we have $81 \equiv 13$ and $1 \equiv 1 \pmod{34}$ in fact it is the first of the two expressions that must be used. So we get $68^2 + 1054^2 = 34^2 \times 5 \times 193$, and cancelling 34^2 gives $2^2 + 31^2 = 5 \times 193$. Now reducing the numbers on the left hand side modulo 5 tells us that $2^2 + 1^2$ must be divisible by 5, and of course it is 5×1. So we deduce that

$$(2^2 + 31^2)(2^2 + 1^2) = 5^2 \times 1 \times 193,$$

giving $(2-62)^2+(4+31)^2 = 5^2 \times 1 \times 193$, and then cancelling 5^2 gives $12^2+7^2 = 193$.

Our next topic is the result known as the *Chinese Remainder Theorem.*

***Theorem:** Suppose that $m_1, m_2, \ldots, m_n$ are pairwise coprime integers. Then for any integers $a_1, a_2, \ldots, a_n$ there exists an integer x such that $x \equiv a_i \pmod{m_i}$ for each $i \in \{1, 2, \ldots, n\}$. If x' and x'' are both solutions of these congruences then $x' \equiv x'' \pmod{m_1 m_2 \cdots m_n}$.

If one can prove this for $n = 2$ then the general case follows easily by induction on n. The idea is that once the case $n = 2$ has been done then we know that the two congruences $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_1 \pmod{m_1}$ can be replaced by a single congruence $x \equiv a \pmod{m_1 m_2}$ for some appropriate a. So we get an equivalent system with one fewer congruence than the original system had. We can then apply the same idea again to reduce the number of congruences once more: since $m_1 m_2$ and m_3 are coprime, the $n = 2$ case tells us that $x \equiv a \pmod{m_1 m_2}$ and $x \equiv a_3 \pmod{m_3}$ are together equivalent to $x \equiv a' \pmod{m_1 m_2 m_2}$ for some a'. The proof given in Walters' book essentially uses this idea.

There is an alternative proof that is perhaps shorter, but does not correspond so closely to the practical procedure for solving simultaneous congruences (as illustrated in the example below). It goes like this. Let $M_i = (m_1 m_2 \cdots m_n)/m_i$.

Then $M_i \in \mathbb{Z}$, and $\gcd(M_i, m_i) = 1$ (since $\gcd(m_j, m_i) = 1$ for all $j \neq i$, by hypothesis). So there exists $N_i \in \mathbb{Z}$ with $M_iN_i \equiv 1 \pmod{m_i}$. But also $M_iN_i \equiv 0 \pmod{m_j}$ for $j \neq i$, since M_i is divisible by all these m_j. So $x = a_1M_1N_1 + a_2M_2N_2 + \cdots + a_nM_nN_n$ satisfies $x \equiv a_j \pmod{m_j}$ for all j, as required. It is clear that the solution is unique modulo $m_1m_2\cdots m_n$, since $x' \equiv x'' \pmod{m_i}$ for all i implies that $x' - x''$ is divisible by all the m_i, and hence by $m_1m_2\cdots m_n$, since they are pairwise coprime.

For example, suppose we wish find a simultaneous solution of $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$, $x \equiv 6 \pmod 9$ and $x \equiv 0 \pmod{11}$. The general solution of the first congruence, by itself, is $x = 3 + 5k$, where $k \in \mathbb{Z}$ is arbitrary. Substituting this into the second congruence gives $3 + 5k \equiv 4 \pmod 7$, or $5k \equiv 1 \pmod 7$. Since the inverse of 5 modulo 7 is 3, this is equivalent to $k \equiv 3 \bmod 7$, or $k = 3 + 7l$ for arbitrary $l \in \mathbb{Z}$, and so the first two congruences are together equivalent to $x = 3 + 5(3 + 3l)$, or $x = 18 + 35l$, where $l \in \mathbb{Z}$ is arbitrary. Now substitute this into the third congruence. We get $18 + 35l \equiv 6 \pmod 9$, or $-l \equiv 6 \pmod 9$, or $l = 3 + 9m$ (where $m \in \mathbb{Z}$). So the first three congruences are together equivalent to $x = 18 + 35(3 + 9m) = 123 + 315m$, where $m \in \mathbb{Z}$. And substituting into the last congruence gives $123 + 315m \equiv 0 \pmod{11}$, or $7m \equiv -2 \pmod{11}$, or $m \equiv 6 \pmod{11}$. So the final solution of our system of congruences is $x = 123 + 315(-6 + 11n) \equiv 2013 \pmod{3465}$.

Lecture 16

To help you with the quiz, here is a procedure for factorizing Gaussian integers. We illustrate with the example $245 + 315i$. Start by taking out all obvious integer factors, to get $n(a+bi)$, with $\gcd(a, b) = 1$. Thus $245+315i = 5(49+63i) = 5.7(7+9i)$. Now work out $(a + bi)(a - bi) = a^2 + b^2$, and factorize it in $\mathbb{Z}$. Thus,

$$(7 + 9i)(7 - 9i) = 7^2 + 9^2 = 130 = 2.5.13.$$

None of the prime factors p will be congruent to 3 modulo 4, since by Question 2 of Assignment 2, if $p \mid a^2 + b^2$ and $p \equiv 3 \pmod 4$ then $p|a$ and $p|b$, whereas in our case $\gcd(a, b) = 1$. So each of the prime factors can be written as a sum of two squares: $p = c^2 + d^2 = (c + di)(c - di)$. Here both $c + di$ and $c - di$ are irreducible Gaussian integers, since they have prime norm. In our example we obtain

$$(7 + 9i)(7 - 9i) = 2.5.13 = (1 + i)(i - i)(2 + i)(2 - i)(3 + 2i)(3 - 2i). \qquad (*)$$

Up to associates, each irreducible factor of $7 + 9i$ must appear amongst the irreducibles on the right hand side, and if $c + di$ is a factor of $a + bi$ then $c - di$ is a factor of $a - bi$. So one of each conjugate pair on the right hand will divide $a + bi$, and we can find which it is by performing a division.† Now

† In fact $1 + i$ and $1 - i$ are associates; so they both divide $7 + 9i$. This does not happen when $N(c + di) > 2$.

$(7+9i)/(2+i) = (7+9i)(2-i)/5 = (23+11i)/5 \notin \mathbb{Z}[i]$. So it must be $2-i$ that divides $7+9i$, and in fact we find that $(7+9i)/(2-i) = (1+5i)$. Now divide $1+5i$ by one of the remaining factors on the right hand side of $(*)$, and continue on until a factorization of $7+9i$ into irreducibles is found. The upshot is that

$$245 + 315i = 5.7(2+i)(3+2i)(1+i).$$

There is one remaining twist: the integer prime factors that we found at the first step are not irreducible in $\mathbb{Z}[i]$ unless they are congruent to 3 modulo 4. In this example, 5 should be factorized as $(2+i)(2-i)$; so the final answer is

$$245 + 315i = 7(2+i)^2(2-i)(3+2i)(1+i).$$

Returning to our discussion of simultaneous congruences, we investigate the case when the moduli are not pairwise coprime. For example, suppose we wish to solve $x \equiv 41 \pmod{45}$ and $x \equiv 32 \pmod{75}$. The idea is to replace each congruence by a system of congruences where the moduli are the prime power divisors of the original modulus. Thus $x \equiv 41 \pmod{45}$ is equivalent to $x \equiv 1 \pmod 5$ and $x \equiv 5 \pmod 9$. Similarly, $x \equiv 32 \pmod{75}$ is equivalent to $x \equiv 2 \pmod 3$ and $x \equiv 7 \pmod{25}$. Now the idea is that two congruences modulo powers of the same prime are either inconsistent or can be reduced to a single congruence (modulo the higher of the two powers). Thus $x \equiv 2 \pmod 3$ is a consequence of $x \equiv 5 \pmod 9$, and is therefore redundant. However, $x \equiv 1 \pmod 5$ is incompatible with $x \equiv 7 \pmod{25}$. It follows that this system of congruences has no solution. By way of contrast, consider now the system $x \equiv 41 \pmod{45}$ and $x \equiv 56 \pmod{75}$. These give $x \equiv 1 \pmod 5$, $x \equiv 5 \pmod 9$, $x \equiv 6 \pmod{25}$ and $x \equiv 2 \pmod 3$. In this case both congruences modulo the lower powers of the two primes are redundant, and so the original system is equivalent to $x \equiv 5 \pmod 9$ and $x \equiv 6 \pmod{25}$. By the procedure described in Lecture 15 we easily discover that the solution is $x \equiv 131 \pmod{225}$.

To understand the Chinese Remainder Theorem better, it is helpful to use a concept from general algebra: that of a *homomorphism*. If n is a fixed positive integer, then every integer may be considered as an integer modulo n. What this really means is that there is a function $f\colon \mathbb{Z} \to \mathbb{Z}_n$; this function is usually called "reduction modulo n". The crucial thing about this function is that the arithemetic operations of addition and multiplication can be performed before or after reduction modulo n, and the final answer is unaltered. That is, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all a, $b \in \mathbb{Z}$.[‡] For example, let $n = 5$ and suppose that $a = 14$ and $b = 8$. Then $f(ab) = f(112) = 2 \in \mathbb{Z}_5$, and $f(a)f(b) = 4 \times 3 = 12 = 2$ (in $\mathbb{Z}_5$).

Whenever m and n are integers such that $n|m$ then there is a reduction mod n homomorphism $\mathbb{Z}_m \to \mathbb{Z}_n$. For example, there is a function $f\colon \mathbb{Z}_{15} \to \mathbb{Z}_5$ given by

[‡] A homomorphism is, by definition, a function satisfying these two equations.

reduction modulo 5. Its values on the various elements of $\mathbb{Z}_{15}$ are given by the following table.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f(k)$	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

This only works because $a \equiv b \pmod{15}$ implies $a \equiv b \pmod 5$. There is no reduction mod 5 map from $\mathbb{Z}_{16}$ to $\mathbb{Z}_5$ since, for example, 1 and 17 are the same modulo 16 but different modulo 5. So reduction mod 5 is not well-defined for elements of $\mathbb{Z}_{16}$.

Inspection of the example above shows that for each element of $\mathbb{Z}_5$ there are three elements of $\mathbb{Z}_{15}$ which yield the given element of $\mathbb{Z}_5$ on reduction mod 5. For example, 2, 7 and 12 are the three distinct elements of $\mathbb{Z}_{15}$ which give 2 on reduction mod 5. Now if x is any integer then reducing x mod 15 and then applying the reduction mod 5 map $\mathbb{Z}_{15} \to \mathbb{Z}_5$ will yield the same result as directly reducing x modulo 5. Thus if $x \equiv 2$ modulo 5 then there are exactly three possibilities modulo 15, namely, $x \equiv 2$, 7 or 12 (mod 15). Similarly, as pointed out in one of the examples above, $x \equiv 1 \pmod 5$ and $x \equiv 7 \pmod{25}$ are not compatible: the 5 elements of $\mathbb{Z}_{25}$ that reduce to 1 (mod 5) are 1, 6, 11, 16 and 21.