Week 7 Summary

Lecture 13

Suppose that p and q are integers with $\gcd(p,q)=1$ (so that the fraction p/q is in its lowest terms) and $0<p<q$ (so that $0<p/q<1$), and suppose that q is not divisible by 2 or 5. Then $\gcd(q,10)=1$, and by the Fermat-Euler Theorem there exists a number k such that $10^k\equiv 1 \pmod{q}$. So there exists an integer m such that $qm=10^k-1$, and it follows that

$$\frac{p}{q}=\frac{pm}{10^k-1}=\frac{pm}{10^k}+\frac{pm}{10^{2k}}+\frac{pm}{10^{3k}}+\cdots$$

(as one can check by applying the formula for the sum of a geometric series). Now $pm<10^k$; so pm is a number of at most k digits. Indeed, we can write it as a k digit number by inserting leading zeros as required. For example, $3/37=9/111=81/999$, which we can write as $081/999$, and now

$$\frac{081}{999}=\frac{081}{10^3}+\frac{081}{10^6}+\frac{pm}{10^9}+\cdots=.081081081\ldots.$$

In the same way, in the general case, we see that

$$\frac{pm}{10^k-1}=.a_1a_2\ldots a_ka_1a_2\ldots a_ka_1a_2\ldots a_k\ldots,$$

where $a_1a_2\ldots a_k$ is the k-digit representation of the integer pm. Thus the decimal expansion of p/q has non-periodic part of length zero; that is, the first repeating block starts immediately after the decimal point. We have shown this for all fractions with denominator coprime to 10. Conversely, since a periodic decimal with non-periodic part of length zero has the form

$$0.\overline{a_1a_2\ldots a_k}=\frac{a_1a_2\ldots a_k}{99\ldots 9}, \qquad (*)$$

we see that every such number is expressible as a fraction with denominator coprime to 10. Furthermore, the length of the periodic part is the smallest k such that the number can be written in the form $(*)$; that is, it is the least k such that the number is expressible as a fraction whose denominator is 10^k-1. For the number p/q (where $\gcd(p,q)=1$) this is the least k such that 10^k-1 is a multiple of q. In other words, it is the order of 10 modulo q.

Let us now drop the assumption that $\gcd(10,q)=1$ (although we still assume that $\gcd(p,q)=1$). Then we may write $q=2^a5^bq'$, where $\gcd(10,q')=1$, and if we define n to be either a or b, whichever is the larger, then

$$10^n\frac{p}{q}=\frac{2^n5^np}{2^a5^bq'}=\frac{p'}{q'}$$

for some integer p'. So $10^np/q$ is expressible as a fraction whose denominator is coprime to 10. And n is the least integer with this property: if we instead multiply p/q by some smaller power of 10 then at least one 2 or 5 will remain in the denominator. So n is the least integer such that in the decimal expansion of $10^n p/q$ the first repeating block starts immediately after the decimal point (since the decimal expansions with this property correspond exactly to fractions with denominator coprime to 10). But since multiplying by 10^n just corresponds to shifting the decimal point n places, it is clear that the length of the non-periodic part of a repeating decimal α is the least n such that $10^n\alpha$ has non-periodic part of length zero.

To summarize the above, for a fraction p/q in its lowest terms, the length of the non-periodic part of the decimal expansion is $\max(a, b)$, where 2^a and 5^b are the powers of 2 and 5 in the prime factorization of q, and the length of the periodic part is the order of 10 modulo q', where q' is the part of q that is coprime to 10. (That is, $q = 2^a 5^b q'$.)

We address now the question of whether -1 is a square in $\mathbb{Z}_p$, where p is a prime. Note that in $\mathbb{Z}_{17}$ we have $4^2 = 16 = -1$; so -1 is a square. But -1 is not a square in $\mathbb{Z}_{19}$, as one can easily check by computing k^2 for all k from 1 to 18, reducing the answers modulo 19. The crucial difference turns out to be that 17 is congruent to 1 mod 4, whereas 19 is congruent to 3 mod 4. We need to prove some preliminary results.

***Lemma:** If $x^2 \equiv 1 \pmod{p}$, where p is prime, then $x \equiv \pm 1 \pmod{p}$.

***Wilson's Theorem:** Let n be an integer greater than 1.
(a) If n is prime then $(n-1)! \equiv -1 \pmod{n}$.
(b) If n is not prime then $(n-1)! \not\equiv -1 \pmod{n}$.

The second part of this is clear, since if n is not prime then we may write $n = ab$ with a, $b \in \{1, 2, \ldots, n-1\}$, and then a and b are both divisors of $(n-1)!$. So they cannot be divisors of $(n-1)! + 1$, and this certainly means that n cannot be a divisor of $(n-1)! + 1$. So $(n-1)! \not\equiv -1 \pmod{n}$.†

The more important part of the theorem, part (a), is proved in all of the reference books listed in the handbook.

Lecture 14

***Proposition:** Let p be an odd prime. Then -1 is a square modulo p if and only if $p \equiv 1 \pmod{4}$.

Note that if $x^2 \equiv -1 \pmod{p}$ then $\mathrm{ord}_p(x) = 4$, and in view of the Euler-Fermat Theorem this implies that $4 \,|\, \varphi(p)$. Bur $\varphi(p) = p - 1$, since p is prime, and so $4 \,|\, p - 1$. That is, $p \equiv 1 \pmod{4}$.

† Indeed, if we can write $n = ab$ with $a \neq b$, and a, $b \in \{1, 2, \ldots, n-1\}$, then $n = ab$ is a divisor of $(n-1)!$. So $(n-1)! \equiv 0 \pmod{n}$. This applies to all composite numbers except squares of primes, and even then we can still conclude that $(n-1)! \equiv 0 \pmod{n}$, since $p^2 | p(2p)$, and $p(2p) | (p^2 - 1)!$, except for the one case $p = 2$. Observe that $3! \equiv 2 \pmod{4}$; for all composite numbers $n > 4$ we have $(n-1)! \equiv 0 \pmod{n}$.

For the converse we show that if $p \equiv 1 \pmod 4$ then in fact $x = ((p-1)/2)!$ is a solution of $x^2 \equiv -1 \pmod p$. The proof uses Wilson's Theorem. To illustrate the idea, suppose first that $p = 17$. Wilson's Theorem says that $16! \equiv -1 \pmod{17}$. But since the numbers 9, 10, 11, ... 16 are congruent modulo 17 to the numbers -8, -7, -6, ... -1, we see that

$$\begin{aligned} 16! &= 1 \times 2 \cdots \times 8 \times 9 \times 10 \times \cdots \times 16 \\ &= 1 \times 2 \cdots \times 8 \times (-8) \times (-7) \times \cdots \times (-1) \\ &= (-1)^8 (8!)^2, \end{aligned}$$

and so $(8!)^2 \equiv -1 \pmod{17}$. The general proof is no more difficult: if $p = 4k+1$ then we have

$$\begin{aligned} -1 &= 1 \times 2 \times \cdots (2k)(2k+1) \cdots (p-2)(p-1) \\ &\equiv 1 \times 2 \times \cdots (2k)(-2k) \cdots (-2)(-1) \\ &= (-1)^{2k}((2k)!)^2 \\ &= ((2k)!)^2. \end{aligned}$$

As a method of finding a solution of $x^2 \equiv -1 \pmod p$, calculating $x = ((p-1)/2)!$ is not particularly good, since it requires performing $(p-1)/2$ multiplications. It would take no more work to calculate x^2 for each x from 1 to $(p-1)/2$, until one is found that is a solution. We give an example illustrating a method, due to Gauss, which reduces the amount of work involved in finding $\sqrt{-1}$ in $\mathbb{Z}_p$.

Consider the prime $p = 821$ (which is congruent to 1 modulo 4), and suppose that x is an integer such that $x^2 + 1$ is a multiple of 821. Reducing x modulo 821 allows us to assume that $-410 \le x \le 410$, and replacing x by $-x$ if need be gives $0 < x \le 410$. For some integer k we have

$$821k = x^2 + 1 \tag{\$}$$

and since $|x| \le 410$ we have $k = (x^2+1)/821 < (410^2+1)/821 < 410^2/820 = 205$. So the integers from 1 to 204 are the only values of k we need consider in the equation ($). We now set about reducing the number of possibilities by looking at ($) modulo various small numbers.

First, we have $2k \equiv 821k \equiv x^2 + 1 \pmod 3$, and since 0 and 1 the only squares modulo 3 it follows that $2k \not\equiv 0 \pmod 3$. So from the list of possible values for k we can eliminate the multiples of 3. This reduces the number of possibilities from 204 to 136. Similarly, since we have $k \equiv 821k \equiv x^2 + 1 \equiv 1$ or $2 \pmod 4$, we can eliminate values of k that are congruent to 0 or 3 modulo 4. This further halves the number of possibilities, reducing it to 68. For any odd prime q the number of possible values for $x^2 + 1$ modulo q is $(q+1)/2$, which is about half the size of $\mathbb{Z}_q$. So considering the equation modulo q is likely to approximately halve the number of possible values for k.

Let us do this carefully. We have established that k nust be congruent to 1 or 2 modulo 3 and to 1 or 2 modulo 4. These facts can be combined to say that k is

congruent to 1, 2, 5 or 10 modulo 12. We have $k \equiv 821k \equiv x^2 + 1 \pmod 5$, and so $k \equiv 1$, 2 or 0 (mod 5). Combined with our previous information this tells us that modulo 60 there are just 12 possibilities for k: they are 1, 2, 5, 10, 17, 22, 25, 26, 37, 41, 46 and 50. We also have $2k \equiv 821kequiv1$, 2, 3 or 5 (mod 7), and so $k \equiv 1$ 4 5 or 6 (mod 7). Let us now write down explicitly all the possibilities that remain. They are 1, 5, 22, 25, 26, 41, 46, 50, 61, 62, 82, 85, 97, 106, 110, 125, 130, 137, 145, 146, 166, 181, 190, 197 and 202. It is by now feasible to compute $821k - 1$ for all these values of k until one is found for which the answer is a square. Or we can continue eliminating possibilities by the same method we have been using. Note also that if q is a prime that is congruent to 3 modulo 4 then $x^2 + 1$ cannot be congruent to 0 modulo q; so $821k$ cannot be divisible by any such q. We may therefore eliminate from our list of possible k's any number that has a prime factor congruent to 3 modulo 4. This gets rid of 22, 46, 62, 110, 145, 166 and 190.
We have $8k \equiv 1$, 2, 5, 10, 6 or 4 (mod 11), and so $k \equiv 7$, 3, 2, 4, 9 or 6 (mod 11). And $2k \equiv 1$, 2, 5, 10, 4, 0 or 11 (mod 13); so $k \equiv 6$, 1, 9, 5, 2, 0 or 12 (mod 13). Our possibilities for k now are 25, 26, 61, 97, 106, 130 and 145. If you have a calculator to hand, then by this stage you will certainly use it to find which value works. But I do not have one to hand. Modulo 17 the possible values for $x^2 + 1$ are 1, 2, 5, 10, 0, 9, 3, 16 and 14. If $k = 25$ then $821k \equiv 5 \times 8 \equiv 6$, which is not in the list. If $k = 26$ then $821k \equiv 45 \equiv 8$, also impossible. If $k = 61$ then $821k \equiv 50 \equiv 16$, which is possible. If $k = 97$ then $821k \equiv 9$, possible. If $k = 106$ then $821k \equiv 3$, possible. If $k = 130$ then $821k \equiv 55 \equiv 4$, impossible. If $k = 145$ then $821k \equiv 45 \equiv 11$, impossible. We are down to 61, 97 or 106. Modulo 19 the corresponding values of $821k$ are 16, 8 and 6. Now 16 is not a possible value for $x^2 + 1$ modulo 19, but 8 and 6 are possible. So, it is 97 or 106. If $k = 97$ then $821k \equiv 16 \times 5 \equiv 11 \pmod{23}$. Is 10 a square mod 23? The squares mod 23 are 0, 1, 4, 9, 16, 2, 13, 3, 18, 12, 8 and 6. So 97 is eliminated, and k must be 106. A quick check reveals that $821 \times 106 = 87026 = 295^2 + 1$. So $295^2 \equiv -1 \pmod{821}$. The amount of writing involved in the above explanation is significantly greater than the amount of actual calculation involved.

We can use the fact that -1 is a square modulo p whenever p is a prime congruent to 1 modulo 4 to prove that every such prime is a sum of two squares. (We foreshadowed this result in Lecture 10, and it completes the description of irreducibles of $\mathbb{Z}[i]$.) The point is that if p is not a sum of two squares then p is an irreducible element of $\mathbb{Z}[i]$ (see Lecture 10). Given that $p \equiv 1 \pmod 4$, there exists an x such that $p \,|\, x^2 + 1$. So $p \,|\, (x + i)(x - i)$ in $\mathbb{Z}[i]$. Since p is irreducible this implies that either $p \,|\, x + i$ or $p \,|\, x - i$. But this is absurd, since clearly neither $(x + i)/p$ nor $(x - i)/p$ is in $\mathbb{Z}[i]$ (as the imaginary parts of these two numbers are $\pm(1/p)$, which are not integers).
It is worth noting that the a and b such that $p = a^2 + b^2$ are unique (up to order and sign), since $p = (a+bi)(a-bi)$ is the factorization of p into irreducibles in $\mathbb{Z}[i]$, and the factorization is unique up to units and associates.

There is a problem of how to actually find a and b in practice, if p is large. For this there is a method discovered by Fermat, which he called the "method of descent". (Very probably, he incorrectly believed that a generalization of this method could be used to prove the result that is now known as Fermat's Last Theorem.)

We illustrate the method for the prime 821. Note that we already know how to express a multiple of 821 as a sum of two squares: we know that

$$295^2 + 1^2 = 821 \times 106. \tag{A}$$

The aim is to "descend", and express a smaller multiple of 821 as a sum of two squares. We look at the equation (A) modulo 106. Since $295 \equiv (-23) \pmod{106}$ we have that $(-23)^2 + 1^2 \equiv 0 \pmod{106}$. Evaluating the left hand side explicitly, and dividing by 106, we find that

$$(-23)^2 + 1^2 = 530 = 5 \times 106. \tag{B}$$

I strongly recommend that when doing one of these examples, you make sure that the terms on the left hand side of equation (B) are kept in the same order as the terms on the left hand side of equation (A) to which they correspond. In the above example, the terms 295^2 and $(-23)^2$ correspond since $295 \equiv -23 \pmod{106}$. Note also that I have retained the minus sign, even though $(-23)^2$ is, of course, the same as 23^2. This is to ensure that the next step works out correctly.

We multiply equations (A) and (B), obtaining

$$(295^2 + 1^2)((-23)^2 + 1^2) = 821 \times 5 \times 106^2,$$

and use the formula $(a^2 + b^2)(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2$. So we obtain

$$(295 \times 1 - 1 \times (-23))^2 + (295 \times (-23) + 1 \times 1)^2 = 5 \times 821 \times 106^2.$$

Do not evaluate the right hand side! We want it in factorized form. The point is that both the squared factors on the left hand side are guaranteed to be divisible by 106^2, and so 106^2 will cancel from the equation. Indeed, $295 + 23 = 318 = 3 \times 106$, and $-295 \times 23 + 1 = -6784 = -64 \times 106$. So we now have

$$3^2 + 64^2 = 821 \times 5, \tag{A$'$}$$

and we have completed one descent.

Modulo 5 equation (rmA') gives $(-2)^2 + (-1)^2 \equiv 0$, and computing the left hand side exactly yields

$$(-2)^2 + (-1)^2 = 1 \times 5. \tag{B$'$}$$

Multiplying (A$'$) and (B$'$) gives

$$(3^2 + 64^2)((-2)^2 + (-1)^2) = 821 \times 5^2,$$

and so

$$(3 \times (-1) - 64 \times (-2))^2 + (3 \times (-2) + 64 \times (-1))^2 = 821 \times 5^2.$$

Now because we made sure that the expressions on left hand sides (A$'$) and (B$'$) are identical modulo 5 it is guaranteed that 5^2 will cancel from this. Indeed $(-3 + 128) = 25 \times 5$ and $-6 - 64 = -14 \times 5$, and so

$$25^2 + 14^2 = 821,$$

expressing 821 as a sum of two squares, as desired.