9. NINTH LECTURE : 17/11

We continue with applications of the algebraic tools developed in the last few lectures.

Proposition 9.1. *Let p be a prime. Then the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

Proof. If $p = 2$ then $x = 1$ is a solution. Now suppose p is an odd prime. If $x^2 \equiv -1 \pmod{p}$ then, considered as an element of the group $\mathbb{Z}_p^*$, x has order 4. But this group is cyclic of order $p-1$, hence has an element of order 4 if and only if $4|p-1$, i.e.: if and only if $p \equiv 1 \pmod{4}$. □

We give two nice applications of this proposition. The first is another special case of Dirichlet's Theorem :

Proposition 9.2. *There are infinitely many primes congruent to 1 (mod 4).*

Proof. As with Theorem 7.2, the basic idea is to suitably modify Euclid's original argument (Theorem 1.2). We thus suppose that there are only finitely many primes congruent to 1 (mod 4), and list them all as $p_1, ..., p_n$. This time we consider the number

$$T := \left(2 \cdot \prod_{i=1}^{n} p_i\right)^2 + 1. \tag{9.1}$$

Clearly T is not divisible by any p_i. It is an odd number so all of its prime factors are odd. Let p be a prime factor of T. I claim that $p \equiv 1 \pmod{4}$. For consider the number $x = 2 \cdot \prod_{i=1}^{n} p_i$. If $p|T$ then $p|x^2+1$, which implies that $x^2 \equiv -1 \pmod{p}$. By Proposition 9.1, this means that $p \equiv 1 \pmod{4}$, as claimed. Since p is not on our list, we have a contradiction which completes the proof. □

A more impressive application of Proposition 9.1 is the following theorem of Fermat :

Theorem 9.3. *Let p be a prime. Then there exist integers x, y such that*

$$x^2 + y^2 = p, \tag{9.2}$$

if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. If $p = 2$ then we have the solutions $x = \pm 1, y = \pm 1$. If $p \equiv 3 \pmod{4}$ then there is clearly no solution, since the square of any integer must be congruent to 0 or 1 modulo 4, so that the sum of two integer squares must be congruent to 0,1 or 2 modulo 4.

Now suppose $p \equiv 1 \pmod{4}$. By Proposition 9.1, there exists an integer x such that $x^2 \equiv -1 \pmod{p}$. Fix such an x and consider the function $f : \mathbb{Z} \to \mathbb{Z}$ given by

$$f(u, v) = u + xv. \tag{9.3}$$

Let $K = [\sqrt{p}]$ so that $K < \sqrt{p} < K + 1$. There are $(K+1)^2 > p$ pairs (u, v) of integers satisfying $0 \leq u, v \leq K$. Thus, by the Pigeonhole Principle, there must be two distinct pairs, say (u_1, v_1) and (u_2, v_2) such that

$$f(u_1, v_1) \equiv f(u_2, v_2) \pmod{p} \Rightarrow (u_1 - u_2) \equiv -x(v_1 - v_2) \pmod{p}. \tag{9.4}$$

Let $a := u_1 - u_2, b := v_1 - v_2$. Since $x^2 \equiv -1 \pmod{p}$, it follows that $a^2 + b^2 \equiv 0 \pmod{p}$. At least one of $a, b \neq 0$, since otherwise the pairs (u_1, v_1) and (u_2, v_2) would coincide. Thus $a^2 + b^2 \neq 0$. But since all of u_1, v_1, u_2, v_2 lie in the interval $[0, K]$, each of a and b must lie in the interval $[-K, K]$. Hence $a^2 + b^2 \leq 2K^2 < 2p$.

To summarise, we have shown that $a^2 + b^2$ is a multiple of p and lies strictly between 0 and $2p$. It follows that $a^2 + b^2 = p$, and the proof is complete. □

Remark 9.4. I find this result surprising from a heuristic viewpoint. Given any $n \in \mathbb{N}$, there are $1 + \lfloor \sqrt{n} \rfloor$ integer squares between 0 and n. Hence there are about n pairs of such squares, and thus no more than about n possible distinct sums of two such squares. But these sums are spread over the whole interval from 0 to $2n$, so only half of them should lie in $[0, n]$. Thus we cannot expect be able to express more than about half of the numbers up to n as sums of two squares. Hence, it is surprising that every single prome congruent to 1 (mod 4) has such a representation. One could, of course, argue that only half of all primes are sums of two squares anyway, since no prime congruent to 3 (mod 4) has such a representation. But I find this heuristic argument unconvincing, since the problem with numbers congruent to 3 (mod 4) is not confined to primes, and it doesn't explain why it should be made up for especially by other primes.

Theorem 9.3 can be extended to non-primes. Before stating the result, we need a lemma :

Lemma 9.5. *The set of integers which can be expressed as a sum of two squares is closed under multiplication.*

Proof. This is a direct consequence of the algebraic identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ab + bc)^2. \tag{9.5}$$

The 'best' way to think about this identity is as follows : consider the complex numbers

$$z_1 := a + bi, \quad z_2 := c + di. \tag{9.6}$$

Then (9.5) is equivalent to the statement that[1]

$$|z_1 z_2| = |z_1||z_2|. \tag{9.7}$$

□

Notation. The notation $p^\alpha || n$ means that p^α is the highest power of the prime p which divides the integer n, i.e.: $p^\alpha | n$ and $p^{\alpha+1} \nmid n$.

Theorem 9.6. *Let $n \in \mathbb{N}$. Then there exist integers x, y satisfying $x^2 + y^2 = n$ if and only if, in the prime factorisation of n, every prime congruent to 3 (mod 4) appears to an even power.*

Proof. Lemma 9.5 is easily seen to imply the sufficiency of the condition in the theorem since note that, if $n \in \mathbb{N}$ is a perfect square, say $n = m^2$, then $n = 0^2 + m^2$ is a valid representation of n as a sum of two squares.

[1] More abstractly, (9.7) asserts that the ordinary absolute value function for complex numbers induces a *norm* in the algebraic number field $\mathbb{Q}(i)$, the so-called field of *Gaussian numbers*.

We will prove the necessity by a contradiction argument[2]. Suppose n is a sum of two squares and that $p^{2k+1}||n$ for some prime $p \equiv 3 \pmod 4$ and $k \geq 0$. Let $n = x^2 + y^2$, say. Then $x^2 + y^2 \equiv 0 \pmod p$. If y were not divisible by p, this would imply that

$$(xy^{-1})^2 \equiv -1 \pmod p, \tag{9.8}$$

where y^{-1} denotes the multiplicative inverse of y in $\mathbb{Z}_p^*$. Eq. (9.8) would contradict Proposition 9.1. Thus $p|y$ and, by a similar argument, $p|x$. Let $x = px_1$, $y = py_1$. Then $x_1^2 + y_1^2 = n_1$, where $n_1 = n/p^2$ and thus $p^{2(k-1)+1}||n_1$.

We can now iterate the arguments of the previous paragraph to produce a non-ending sequence of integers $n_1, n_2, ...$ divisible by lesser and lesser, but always odd, powers of the prime p. Clearly, this is ridiculous so the proof is complete. □

[2]The method of infinite descent.

10. TENTH LECTURE : 19/11

There are two conceptually quite distinct ways of looking at Theorem 9.6 from last day, which take one down different, but well-travelled paths.

ALTERNATIVE 1 : See it as a result in *additive* number theory, i.e.: roughly speaking, as a statement about expressing numbers as sums of other numbers.
ALTERNATIVE 2 : See it as a result about *quadratic forms*.

In the next few lectures, we will be concerned with exploring Alternative 2. First of all, though, I want to state some major results and open problems one encounters if one explores Alternative 1, and later in the course I will give a general introduction to additive number theory.

Theorem 9.6 tells us which non-negative integers can be expressed as sums of two squares. Since the answer is 'not all', it is very natural to ask what happens if we allow longer sums. There are the following two famous results :

Theorem 10.1. (Gauss) *A non-negative integer is a sum of three squares if and only if it is not of the form* $4^k m$, *where* $m \equiv 7 \pmod 8$.

It is easy to check that the conditions of the theorem are necessary (see Homework 3). Proof of sufficiency is highly non-trivial, however, and beyond the scope of this course. For a proof, see for example the book

J.-P. Serre, *A Course in Arithmetic (Cours d'Arithmétique)*, Springer GTM Series.

Theorem 10.2. (Lagrange 1770) *Every non-negative integer is a sum of four squares.*

This is actually easier to prove than Gauss' theorem, and we will do so later on. Note that Theorems 10.1 and 10.2 are still concerned with quadratic forms. The step beyond quadratic forms, and deeper into the realm of additive number theory, was taken by Waring who, also in 1770, reputedly sent a handwritten letter to Euler containing the following conjecture :

Waring's Problem. *For every* $k \in \mathbb{N}$, *there exists an integer* $g(k)$ *such that every non-negative integer can be written as a sum of* $g(k)$ *perfect* k*:th powers of non-negative integers.*

Note that Theorems 10.1 and 10.2 together imply that $g(2) = 4$. Trivially, $g(1) = 1$. Not much else was known until 1909, when Hilbert proved the conjecture for all k. Hilbert's proof is 'purely combinatorial', i.e.: he doesn't use analysis, but is long and complicated. An alternative proof, using Fourier analysis, was provided by Hardy and Littlewood in the 1920s. This proof is far better known since their method, now known as the *Hardy-Littlewood circle method*, has proved far more influential than that of Hilbert. It is one of the key tools of analytic number theory to this day, and some of the most famous results in the subject have been obtained using it, especially problems of an additive nature. I wish to state two particularly famous results. The first concerns sums of primes :

Theorem 10.3. (Vinogradov 1937) *Every sufficiently large odd number is a sum of three primes.*

It is not known whether every odd number greater than 7 is a sum of three primes. Though Vinogradov's theorem leaves only a finite collection of numbers to check, the number that comes out of his analysis, as the bound up to which one has to check, is really enormous and far out of the range of current hardware and software.

Note that Theorem 10.3 implies that every sufficiently large number is a sum of at most 4 primes. Thus, there is certainly some $k > 0$ such that every number greater than one is a sum of no more than k primes. This fact was actually proven by Schnirelmann already in 1930 by combinatorial means. Schnirelmann's methods have actually had a lasting impact on additive number theory and we may say more about them later in the course. Regarding sums of primes, however, his approach gives a totally unrealistic value of k and seems to reach a dead-end. What one expects to be the 'truth' is contained in the following famous open problem :

Goldbach's Conjecture. *Every even number greater than two is a sum of two primes. Equivalently, every number greater than one is a sum of at most three primes.*

It is known that Goldbach's conjecture is true for 'most' numbers. Mopre precisely, in 1938 van der Corput applied Vinogradov's methods to prove

Theorem 10.4. *For an integer $n > 1$, let A_n denote the number of even integers among $\{4, 6, ..., 2n\}$ which can be expressed as a sum of two primes. Then*

$$\lim_{n\to\infty} \frac{A_n}{n} = 1. \tag{10.1}$$

Note that the proof of this result is totally non-constructive, i.e.: it doesn't tell us anything about whether any specific even number is a sum of two primes or not. It is also curious that the circle method, as applied by Vinogradov, gets one so close to Goldbach's Conjecture, but just seems to fall short at the last hurdle !

The second major result I wish to mention which was established using the Hardy-Littlewood method concerns integer partitions.

Definition. Let $n \in N$. A *partition* of n is a set $\{a_1, ..., a_k\}$ of positive integers such that

$$n = a_1 + \cdots + a_k. \tag{10.2}$$

Note that we do not distinguish between partitions in which the same terms have just been reordered. The *partition function* $p(n)$ counts the number of partitions of n.

Example. $p(5) = 7$ and all the partitions of 5 are

$$5,\ \ 4+1,\ \ 3+2,\ \ 3+1+1,\ \ 2+2+1,\ \ 2+1+1+1,\ \ 1+1+1+1+1. \tag{10.3}$$

Hardy and Ramanujan established an amazing asymptotic formula for the partition function. In its simplest form it states that

Theorem 10.5.

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4\sqrt{3}\,n}. \tag{10.4}$$

Remark 10.6. Let $c(n)$ denote the number of *compositions* of a positive integer n, i.e.: the number of solutions to (10.1), where this time we distinguish between re-ordered solutions. It can be shown by a clever one-line argument (see Homework 3) that $c(n) = 2^{n-1}$. Note, in particular, that the function $c(n)$ grows exponentially, whereas $p(n)$ exhibits so-called *intermediate growth*, i.e.: faster than polynomial but slower than exponential.

Remark 10.7. It is known that the function $g(k)$ grows exponentially with k, but this is because, for each k, there are a finite number of relatively small numbers which are particularly awkward to write as a sum of k:th powers (see Homework 3). More interesting are thus the functions $G(k)$, defined as the smallest number of k:th powers needed to represent any sufficiently large number. The only values of this function that are known are $G(1) = 1$, $G(2) = 4$ and $G(4) = 16$, and the computation of the function for other k remains an active area of research.

For an in-depth introduction to the Hardy-Littlewood method and its application to Waring's Problem, Goldbach's Problem, partitions and other additive problems, I recommend the following texts :

1. R.C. Vaughan, *The Hardy-Littlewood Method (2nd edition)*, Cambridge University Press (1997).
2. G.H. Hardy, *Trois Problèmes célèbres de la theorie des nombres*, Les Presses Universitaires de France (1931).

The book *Introduction to the Theory of Numbers*, also by Hardy, contains a lot of information on 'elementary' approaches to these famous additive problems. Another good reference for elementary approaches is *Elementary Number Theory*, by Melvyn Nathanson.

In the next lecture, we will start exploring what I identified as Alternative 2 above.

11. Eleventh Lecture : 19/11

We prepare the ground for our discussions of both quadratic forms and L-functions with some more algebraic preliminaries.

Definition. Let G be a finite abelian[3] group. A *character* of G is a homomorphism $\chi : G \to \mathbb{C}^*$, where $\mathbb{C}^*$ denotes the multiplicative group of non-zero complex numbers. The collection of all characters of a group G is denoted $\hat{G}$.

Definition. Let $n \in \mathbb{N}$. A complex number ζ satisfying $\zeta^n = 1$ is called an *n:th root of unity*. If $\zeta^n = 1$ but $\zeta^n \neq 1$ for $1 \leq k < n$, then we say that ζ is a *primitive* n:th root of unity. The collection of all n:th roots of unity is denoted μ_n.

Proposition 11.1.

$$\mu_n = \{e^{2\pi ik/n} : 0 \leq k < n\}. \tag{11.1}$$

In particular, $|\mu_n| = n$. μ_n is a subgroup of $\mathbb{C}^*$. The primitive n:th roots of unity are the numbers $e^{2\pi ik/n}$ satisfying GCD$(k, n) = 1$.

Proof. All these statements are pretty obvious. □

Proposition 11.2. *Let G be a finite abelian group of order n and $\chi \in \hat{G}$. Then $\chi(G) \subseteq \mu_n$.*

Proof. Let $g \in G$. Then $g^n = 1_G$, by Lagrange's Theorem. Thus $\chi(g^n) = \chi(1_G)$. Since χ is a homomorphism we have, on the one hand, that $\chi(1_G) = 1$ and, on the other, that $\chi(g^n) = [\chi(g)]^n$. Thus $[\chi(g)]^n = 1$, so $\chi(g) \in \mu_n$, v.s.v. □

Characters can be multiplied pointwise as functions, i.e.: if $\chi_1, \chi_2 \in \hat{G}$, then we can define their 'product' $\chi_1\chi_2$ by

$$(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g). \tag{11.2}$$

Proposition 11.3. *$\hat{G}$ is closed under the multiplication defined above, i.e.: if χ_1 and χ_2 are characters, then so is $\chi_1\chi_2$. Moreover, $\hat{G}$ is a finite abelian group under this operation.*

Proof. It is easy to check that if χ_1 and χ_2 are both characters, then so is $\chi_1\chi_2$. The function which sends every element of G to 1 is an identity element for this multiplication. Finally, an inverse to the character χ is the function

$$\chi^{-1}(g) := \frac{1}{\chi(g)} = \overline{\chi(g)}. \tag{11.3}$$

Thus $\hat{G}$ is an abelian group. It is finite, since both the domain and range of any character are contained inside fixed finite sets, by Proposition 11.2. □

Notation. The identity element in $\hat{G}$ is called the *trivial character* and is often denoted χ_0.

An important fact is the following :

[3]The definition makes sense for any group, finite or infinite, abelian or not, but we confine attention to abelian groups for simplicity, since only such groups will actually be considered.

Theorem 11.4. *For any finite abelian group G, the groups G and $\hat{G}$ are isomorphic as abstract groups*[4].

Proof. (sketch) By the Fundamental Theorem of Finite Abelian Groups, any finite abelian group can be decomposed as a direct product of cyclic groups. Suppose

$$G = < g_1 > \times \cdots \times < g_r > \cong C_{n_1} \times \cdots \times C_{n_r}. \tag{11.4}$$

For each $s = 1, ..., r$, let $\chi_s : G \to \mathbb{C}^*$ be the unique character defined by the conditions

$$\chi_s(g_k) = \begin{cases} e^{2\pi i/n_s}, & \text{if } k = s, \\ 1, & \text{if } k \neq s. \end{cases} \tag{11.5}$$

Then it is not hard to check that χ_s has order n_s in $\hat{G}$ and that

$$\hat{G} \cong < \chi_1 > \times \cdots \times < \chi_r > \cong C_{n_1} \times \cdots \times C_{n_r} \cong G. \tag{11.6}$$

□

Remark 11.5. Given a basis for G as in (11.4), the corresponding basis for $\hat{G}$ defined by (11.5) is called the *dual* basis. In fact, the group $\hat{G}$ is sometimes called the *dual group* of G.

Definition. A character χ of a group G is said to be *real* if $\chi(G) \subseteq \mathbb{R}$. By Proposition 11.2, it is then the case that $\chi(G) \subseteq \{\pm 1\}$.

In number theory, the groups we are interested in first and foremost are the groups $\mathbb{Z}_n^*$.

Definition. A character of the group $\mathbb{Z}_n^*$ is called a *Dirichlet character* modulo n. A function $\chi : \mathbb{Z} \to \mathbb{C}$ is called an *extended Dirichlet character* modulo n if the following three conditios are satisfied :

(i) $\chi(x) = \chi(y)$ whenever $x \equiv y \pmod{n}$, so that χ can be considered as a function from $\mathbb{Z}_n$ to $\mathbb{C}$,

(ii) as such, the restriction of χ to $\mathbb{Z}_n^*$ is a Dirichlet character modulo n,

(iii) $\chi(x) = 0$ whenever $\text{GCD}(x, n) > 1$.

Suppose $n = p$, a prime. Since $\mathbb{Z}_p^*$ is cyclic, there is only one non-trivial real Dirichlet character modulo p. This is called the *Legendre symbol* modulo p and is denoted $\left(\frac{\cdot}{p}\right)$. The corresponding extended character is given explicitly by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a, \\ 1, & \text{if } p \dagger a \text{ and the congruence } x^2 \equiv a \pmod{p} \text{ has a solution,} \\ -1, & \text{otherwise.} \end{cases} \tag{11.7}$$

The elements $a \in \mathbb{Z}_p^*$ for which $\left(\frac{a}{p}\right) = 1$ are called the *quadratic residues* modulo p.

[4]For a general finite group G we have an isomorphism $\hat{G} \cong G/G'$, where G' is the commutator subgroup of G.

We now turn to quadratic forms. Inspired perhaps by scattered observations of Fermat like Theorem 9.3, Gauss initated a rigorous study of Diophantine equations

$$f(x_1, ..., x_k) = n, \tag{11.8}$$

where f is a so-called *quadratic form*, i.e.: a homogeneous polynomial of degree 2. Thus the general form of f is

$$f(x_1, ..., x_k) = \sum_{i=1}^{k} a_{ii}x_i^2 + \sum_{1\le i<j\le k} a_{ij}x_i x_j, \quad a_{ij} \in \mathbb{Z}. \tag{11.9}$$

He developed a very comprehensive theory for forms in 2 variables (so-called *binary forms*), though it would take another hundred years before a correspondingly comprehensive theory was worked out satisfactorily for arbitrary forms. Gauss wrote a book on arithmetic, *Disquitiones Arithmeticae*, when in his mid-twenties, and a large part of this text is concerned with presenting his theory of binary quadratic forms. Gauss' main insight was that, just as was the case in Theorem 9.3 for the form $f(x, y) = x^2 + y^2$, the question of existence of, and even the number of, solutions to (11.8) could essentially be reduced to solving congruences[5]. I have decided not to go into the details of Gauss' theory in this course, as there are other things I want to do and it would take a significant amount of time. But see, for example, my lecture notes from 2004 for a comprehensive account. I will confine myself to some basic observations about quadratic congruences, without indicating the deeper connections with quadratic equations.

In fact, I will only talk about the basic one-variable quadratic congruence modulo a prime (for non-prime moduli, see Homework 3) :

$$ax^2 + bx + c \equiv 0 \pmod{p}, \quad p \text{ prime}, p \nmid a. \tag{11.10}$$

Now, since $\mathbb{Z}_p$ is a field, the usual procedure for solving a quadratic equation in $\mathbb{C}$ remains valid in the present context, so we get an explicit formula for the solutions when they exist, namely

$$x \equiv \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \pmod{p}. \tag{11.11}$$

In particular, solutions exist if and only if $b^2 - 4ac$ is a square in $\mathbb{Z}_p$. More precisely,

Proposition 11.6. *If p is an odd prime, then the number of solutions to (11.10) in $\mathbb{Z}_p$ is $1 + \left(\frac{b^2-4ac}{p}\right)$.*

Proof. One needs to check that if $\left(\frac{\xi}{p}\right) = 1$ then the congruence $x^2 \equiv \xi \pmod{p}$ has exactly two solutions in $\mathbb{Z}_p$. This is easily seen to reduce to checking that

$$x^2 \equiv y^2 \pmod{p} \Leftrightarrow x \equiv \pm y \pmod{p}. \tag{11.12}$$

To see this, the left-hand side implies that $p|x^2 - y^2 \Rightarrow p|(x - y)(x + y) \Rightarrow p|x - y$ or $p|x + y$, since p is prime, hence $x \equiv \pm y \pmod{p}$, as desired. □

[5]The ultimate expression of this philosophy, for quadratic forms in an arbitrary number of variables, is the so-called *Hasse principle* which, roughly speaking, states that the existence of solutions to (11.8) can be determined by examining the equation modulo only a finite number of prime powers, depending only on the coefficients in f. A precise statement is the renowned *Hasse-Minkowski Theorem*, which is too technical to state here. See Serre's book, *A Course in Arithmetic*, for an account of this theory.

Thus deciding whether or not a quadratic congruence to a prime modulus has a solution reduces to computing a Legendre symbol[6]. Efficient methods for computing Legendre symbols were developed in historical order by Euler, Gauss and Jacobi. It is Gauss' result which was the main breakthrough. His so-called *Law of Quadratic Reciprocity* states the following :

Theorem 11.7. *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}. \tag{11.13}$$

In other words,

$$\left(\frac{p}{q}\right) \neq \left(\frac{q}{p}\right) \quad \textit{if and only if} \quad p \equiv q \equiv 3 \ (\textit{mod}\ 4). \tag{11.14}$$

The proof of this major result, which requires a good deal of effort, will occupy the next one and a half lectures. Before we start with that, I want to illustrate the usefulness of the result with some examples.

Example 1. Proposition 9.1 can be restated as :

$$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p = 2 \text{ or } p \equiv 1 \pmod 4. \tag{11.15}$$

Example 2. Let p be an odd prime. I claim that

$$\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 3. \tag{11.16}$$

To see this, first note that since the Legendre symbol is a character, we have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right). \tag{11.17}$$

Thus, for $\left(\frac{-3}{p}\right) = 1$ to be satisfied, there are two possibilities :

CASE 1 : $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = +1$,
CASE 2 : $\left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = -1$.

First consider Case 1. From Example 1 we must have $p \equiv 1 \pmod 4$. Since $p \not\equiv 3 \pmod 4$, Gauss reciprocity implies that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. But clearly, $\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 3$.

Thus, the conditions of Case 1 are satisfied if and only if both $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$.

Case 2 is analysed similarly. This time, Example 1 tells us that $p \equiv 3 \pmod 4$. Since

[6]Once it is known that $\left(\frac{\xi}{p}\right) = 1$, there is a polynomial-time algorithm for computing $\sqrt{\xi} \pmod p$. See Section 2.2 of Koblitz' book, *A Course in Number Theory and Cryptography*, for an account of this algorithm.

obviously $3 \equiv 3 \pmod 4$, Gauss reciprocity tells us this time that $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$. Thus we again want $\left(\frac{p}{3}\right) = +1$, hence $p \equiv 1 \pmod 3$.

In summary, the conditions of Case 2 are satisfied if and only if both $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$.

Altogether, then, the conditions of either Case 1 or Case 2 are satisfied by an odd prime p if and only if $p \equiv 1 \pmod 3$, as claimed.

We ran out of time, so will continue next day ....

12. Twelvth Lecture : 21/11

Example 2 from the last lecture leads to another special case of Dirichlet's theorem.

Proposition 12.1. *There are infinitely many primes congruent to 1 (mod 3).*

Proof. Similar to that of Proposition 9.2. Assume there are only finitely many such primes and list them all as $p_1, ..., p_n$. Consider this time the number

$$T := \left(2 \cdot \prod_{i=1}^{n} p_i\right)^2 + 3. \tag{12.1}$$

No $p_i = 3$, thus T is not divisible by any p_i. Neither is it divisible by 2 or 3. Let p be a prime divisor of T and set $x := 2 \cdot \prod_{i=1}^{n} p_i$. Then $p|x^2 + 3$ so $x^2 \equiv -3 \pmod{p}$. By Example 2, this implies that $p \equiv 1 \pmod{3}$, but since p is not on our list, we have a contradiction. □

Example 3. *Find all primes p for which $\sqrt{7}$ exists mod p.*

Obviously, we can take $p = 7$. Otherwise, we seek those p for which $\left(\frac{7}{p}\right) = 1$. If $p = 2$, then $\sqrt{7} \equiv 1 \pmod{2}$. Otherwise, p is odd and we can exploit Gauss reciprocity. Since $7 \equiv 3 \pmod{4}$, there are two cases to consider :

Case 1 : $p \equiv 1 \pmod{4}$. Then $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$, so we want $\left(\frac{p}{7}\right) = 1$. One checks by hand that the quadratic residues mod 7 are 1,2 and 4. Thus there are three possibilitites for $p \pmod{7}$. Together with the condition mod 4, this gives (by the CRT) three possibilities mod 28.

Case 2 : $p \equiv 3 \pmod{4}$. Then $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$, so we want $\left(\frac{p}{7}\right) = -1$. The quadratic non-residues mod 7 are 3,5 and 6. So once again we'll have three possibilities mod 28.

In total, we have six possibilities mod 28 :

$p \pmod 4$	$p \pmod 7$	$p \pmod{28}$
1	1	1
1	2	9
1	4	$25 \equiv -3$
3	3	3
3	5	$19 \equiv -9$
3	6	$27 \equiv -1$

So the answer to the question posed is that $\sqrt{7}$ exists mod p if and only if $p = 2$, $p = 7$ or $p \equiv \pm 1, \pm 3$ or $\pm 9 \pmod{28}$.

We now turn to the proof of Theorem 11.7. We will need two preliminary results, *Euler's criterion* and *Gauss' lemma*.

Proposition 12.2. (Euler's criterion) *Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \dagger a$. Then $\left(\frac{a}{p}\right) = +1$ if and only if $a^{(p-1)/2} \equiv +1 \ (mod\ p)$.*

Proof. The group $\mathbb{Z}_p^*$ is cyclic of order $p-1$. Hence an element a of this group is a square if and only if its order divides $(p-1)/2$, in other words, if and only if, considered as an ordinary integer, $a^{(p-1)/2} \equiv 1 \pmod{p}$, v.s.v. □

Remark 12.3. (i) If $\left(\frac{a}{p}\right) = -1$ then $a^{(p-1)/2} \equiv -1 \pmod{p}$.
(ii) Eulers criterion gives an efficient method for computing any individual Legendre symbol, using the square and multiply algorithm. However, it doesn't help us answer the kind of question asked in the examples above, namely, given $a \in \mathbb{Z}$, for which primes p is $\left(\frac{a}{p}\right) = 1$? For that, we'll need Gauss reciprocity (and its extension by Jacobi, as we'll see later).

Theorem 12.4. (Gauss' lemma) *Let p be an odd prime. For each $n \in \mathbf{Z}$, let $[n]$ denote the unique number satisfying $[n] \equiv n \ (mod\ p)$ and $-\frac{1}{2}p < [n] < \frac{1}{2}p$.*

Now let $a \in \mathbb{Z}$ such that $p \dagger a$ and set $a_j = [aj]$ for each $j \in \mathbb{Z}$. Then

$$\left(\frac{a}{p}\right) = (-1)^l \tag{12.2}$$

where

$$l = \#\{j : 1 \leq j \leq \frac{p-1}{2} \text{ and } a_j < 0.\} \tag{12.3}$$

Proof. We evaluate the product

$$P := \prod_{j=1}^{(p-1)/2} aj \pmod{p} \tag{12.4}$$

in two different ways. First, by its' very definition,

$$P = a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right) \left(\frac{p-1}{2}\right)!, \tag{12.5}$$

by Euler's criterion. On the other hand, by definition we also have that

$$P \equiv \prod_{j=1}^{(p-1)/2} a_j. \tag{12.6}$$

Now I claim that, if $j \neq k$, then $a_j \not\equiv \pm a_k \pmod{p}$. For if $a_j \equiv \pm a_k$ then $aj \equiv \pm ak \Rightarrow p|a(j \mp k) \Rightarrow p|j \mp k$. But both j and k lie in the interval $[1, \frac{p-1}{2}]$, so if $j \neq k$, then $|j \mp k| \leq 2 \cdot (\frac{p-1}{2}) = p - 1 < p$, which makes it impossible for this quantity to be divisible by p.

Thus we've established our claim. This implies that the quantities $|a_j|$ are just a permutation of the numbers $1, 2, ..., \frac{p-1}{2}$, as j runs from 1 to $\frac{p-1}{2}$. By definition, l of them are negative. Hence

$$P \equiv \prod_{j=1}^{(p-1)/2} a_j = (-1)^l \cdot \left(\frac{p-1}{2}\right)! \tag{12.7}$$

But (12.2) follows immediately from (12.5) and (12.7). □

Remark 12.5. The number $[n] \in \left(-\frac{p-1}{2}, \frac{p-1}{2}\right)$ such that $n \equiv [n] \pmod{p}$ is called the *numerically least residue* of n modulo p.

Gauss' lemma is of interest in its own right (which is why I called it a theorem). For example, it allows us to calculate the Legendre symbol $\left(\frac{2}{p}\right)$, which is not covered by the reciprocity law.

Corollary 12.6. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \ (\text{mod } 8), \\ -1, & \text{if } p \equiv \pm 3 \ (\text{mod } 8). \end{cases} \tag{12.8}$$

Proof. We take $a = 2$ in Gauss' lemma. Let $j \in [1, \frac{p-1}{2}]$. Then

$$[2j] > 0 \Leftrightarrow 2j \leq \frac{p-1}{2} \Leftrightarrow j \leq \lfloor \frac{p-1}{4} \rfloor.$$

Hence, for $a = 2$, the quantity l in Gauss' lemma is just

$$l = \frac{p-1}{2} - \lfloor \frac{p-1}{4} \rfloor. \tag{12.9}$$

It is now a short but tedious computation to verify that, for any odd number p, the RHS of (12.9) is congruent to $(p^2-1)/8$ modulo 2. This and Gauss' lemma yield the desired result. □

We will finish the proof of the reciprocity law next day.