Introduction to Number Theory

Agata Smoktunowicz

15th January 2019

Lecture 1

A note on authorship

These lecture notes include excerpts from notes written by Prof Tom Lenagan and Dr Mark Grant.

Plan for Lecture 1

1. Well-ordering principle.
2. Division Algorithm.
3. (Extended) Euclidean Algorithm.

Well-ordering principle

Every non-empty set of positive integers contains a least element.

Theorem 1 (Division Algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique pair $q, r \in Z$ such that

$$a = qb + r$$

and $0 \leq r < b$. q is called the quotient and r is called the remainder.

Proof. (Allenby, page 28)

- Assume first that $a > 0$. Let S be the set of all nonnegative integers belonging to $\{a - mb : m \in \mathbb{Z}\}$.
- Then S is non empty, since $a \in S$. By the obvious extension of the well-ordering principle from $\mathbb{N}$ to $\mathbb{N} \cup \{0\}$, S has a least member, which we shall denote by r.
- Thus $r = a - m_1 b$ for some $m_1 \in \mathbb{Z}$. We claim that $r < b$. For otherwise $0 < b \leq r$. It then follows that $a - (m_1 + 1)b = r - b$ is an element in S smaller than the smallest element r of S. This absurdity leads us to conclude that $r < b$.
- Thus m_1 and r are such that $a = m_1 b + r$, where $0 \leq r < b$.

- Assume now that $a < 0$. By the above we can find m, r, such that $-a = mb + r$, where $0 \leq r < b$. Then $a = (-m)b - r$, where $b < r \leq 0$. If $r = 0$ then we are done. If $0 < r < b$ then $a = (-m-1)b + (b-r)$. Clearly $-m-1 \in Z$ and $0 < b - r < b$ if $0 < r$. (If $r = 0$ there is nothing to prove since then $a = (-m)b + r$, where $0 \leq r < b$ immediately).

- Notice that q and r are unique, since if $a = qb + r$ and $a = q'b + r'$ and $0 \leq r < r' < b$ then $(q - q')b = r' - r$ hence $0 < (q - q')b < b$, a contradiction.

Definition. Let $a, b \in \mathbb{Z}$. We say that a divides b, written $a|b$, if there exists $c \in Z$ such that $b = ac$.

Examples. 3|6. 7|49. 19 does not divide 27.

Definition. Let $a, b \in \mathbb{Z}$. Then $0 < d \in \mathbb{Z}$ is a greatest common divisor (gcd) of a and b if:

(i) $d|a$ and $d|b$ (so d is a common divisor of a and b), and

(ii) if c is also a common divisor of a and b then $c|d$.

Exercise. If $a, b, c \in \mathbb{Z}$ are such that $c|a$ and $c|b$ then $c|sa + tb$ for all $s, t \in \mathbb{Z}$.

Proof. Let $a = c \cdot x$ and $b = c \cdot y$ then $sa + tb = c \cdot (sx + ty)$, so $c|sa + tb$.

Theorem 2. Any two integers $a, b \in \mathbb{Z}$ (not both zero) have a unique positive gcd, which we will denote by (a, b) (and sometimes by gcd(a,b)). Furthermore, there exist $s, t \in Z$ such that $(a, b) = sa + tb$.

Proof. The proof will be given in Lecture 2.

Exercise. Let $a, b \in \mathbb{Z}$. Let S be the set of common divisors of a and b, then gcd(a,b) is the largest positive member of S.

Proof. The proof will be given in Lecture 2.

Exercise. Let $a > b > 0$, then the greatest common divisor of a and b is unique.

Proof. At tutorials.

The above Theorem 2 is not constructive - it tells us that (a, b) and the integers s, t exist, but does not tell us how to find them. For this we may use the following (extended) Euclidean algorithm.

(Extended) Euclidean algorithm

- Let $a, b \in \mathbb{Z}$ be such that $a \geq b > 0$. Then by the division algorithm there exist (unique) integers q_1, r_1 such that $a = q_1 b + r_1$, $0 \leq r_1 < b$.

- Assuming that $r_1 > 0$, then we can apply the division algorithm to the pair b, r_1 and get $b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$. If $r_2 > 0$ then we may divide r_1 by r_2, and so on. We obtain a system of equations. In step 1 we obtain

  $$r_1 = q_3 r_2 + r_3,$$

  where

  $$0 \leq r_3 < r_2$$

  In step 2 we obtain:

  $$r_2 = q_4 r_3 + r_4,$$

  where

  $$0 \leq r_4 < r_3$$

- Continuing in this way, we get

  $$r_k = q_{k+2} r_{k+1} + r_{k+2}$$

  where

  $$0 \leq r_{k+2} < r_{k+1}$$

  Notice that the terms in the sequence $b > r_1 > r_2 > ...$ are finite, strictly decreasing and non-negative, hence must eventually be zero. Therefore some $r_{k+2} = 0$ for some k.

- The last non-zero remainder r_{k+1} is the gcd(a,b). Sometimes we can get the zero remainder in the first step-in this case a is divisible by b and then b is the gcd(a,b).

- In Lecture 2 we will show that the last non-zero remainder r_{k+1} is the gcd(a,b).

Exercise. Find the greatest common divisor of 17 and 5.

Solution.

17=**5**·3+**2**

5=**2**·2+ **1**

2=**1**·2+ **0**.

The last non-zero remainder is 1, so gcd(17,5)= 1.

Introduction to Number Theory

Agata Smoktunowicz

18th January 2019

Lecture 2

A note on authorship

These lecture notes include excerpts from notes written by Prof Tom Lenagan and Dr Mark Grant.

Plan for Lecture 2

1. Prove Theorem 2 from Lecture 1.
2. Prove that the Euclidean algorithm always works (i.e. always gives the greatest common divisor of a and b).

Theorem 1. (Division Algorithm) from Lecture 1

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists a unique pair $q, r \in Z$ such that

$$a = qb + r$$

and $0 \leq r < b$. (q is called the quotient, r is called the remainder).

Definition. Let $a, b \in \mathbb{Z}$. Then $0 < d \in \mathbb{Z}$ is a greatest common divisor (gcd) of a and b if:

i $d|a$ and $d|b$ (so d is a common divisor of a and b), and

ii if c is also a common divisor of a and b then $c|d$.

Our first aim for Lecture 2 is to prove Theorem 2.

Theorem 2. Any two integers $a, b \in \mathbb{Z}$ (not both zero) have a unique positive gcd, which we will denote by (a, b). Furthermore, there exist $s, t \in Z$ such that $(a, b) = sa+tb$.

Proof.

- First assume that both a and b are nonzero. Set $S = \{ma + nb > 0 | m, n \in \mathbb{Z}\}$. Note that $|a|, |b| \in S$, so that S is a non-empty set.

- By the well-ordering principle, choose a least element of S and call it d.
- Suppose that $d = sa + tb$ for some $s, t \in \mathbb{Z}$ (this is possible since $d \in S$). Claim: This d is the unique positive gcd of a, b.
- In fact, first, we show that $d|w$ for all $w \in S$. In particular, we will then know that d divides $|a|$ and $|b|$ (as they are in S), and it follows that $d|a$ and $d|b$, so that d is a common divisor of a, b.
- Let $w \in S$, say $w = ma + nb$ for some $m, n \in \mathbb{Z}$. By the division algorithm, there exist $q, r \in Z$ with $w = qd + r$, and $0 \leq r < d$. Note that $r \notin S$, since $r < d$. Suppose that $r \neq 0$. Then $r = w - qd = (m - qs)a + (n - qt)b \in S$, a contradiction. Thus, $r = 0$ and so $d|w$. Thus, d is a common divisor of a, b.
- Next, assume that $c|a$ and $c|b$. Then, by Lemma 1 we know that $c|sa + tb$; that is, $c|d$. Thus, d is a (positive) greatest common divisor of a, b.
- Notice that d is the unique positive gcd. If c is another positive gcd then $d|c$ and $c|d$ so $d = cx$ and $c = dy$, so $c = xyc$, it follows that $x = y = 1$, as otherwise $c < xyc$.

Lemma. (Bezout) Let $a, b \in \mathbb{Z}$ (not both zero). If $d = gcd(a, b)$ then there exists $m, n \in \mathbb{Z}$ with $a \cdot m + b \cdot n = d$.

Proof. Immediate from Theorem 2.

Recall that we sometimes denote $gcd(a, b)$ by (a, b).

Theorem. Let $a, b, c \in \mathbb{Z}$, (a and b not both zero). Then $a \cdot x + b \cdot y = c$ has solutions in integers x, y if and only if $(a, b)|c$.

Proof. If $(a, b)|c$ then $a \cdot m + b \cdot n = c$ for some integers m, n (by the Bezout lemma). Let $c = (a, b) \cdot \alpha$ for some integer α, then $a \cdot m\alpha + b \cdot n\alpha = (a, b)\alpha = c$, as required.

If (a, b) doesn't divide c, then (a, b) divides the left hand side but does not divide the right hand side, so there are no solutions of this equation.

Exercise. Let $a, b \in \mathbb{Z}$ (a and b not both zero). Let Q be the set of common divisors of a and b, then gcd(a,b) is the largest positive member of Q.

Solution. Let d be the largest positive member in Q. By Theorem 2 we know that (a, b) exists. By the definition of the greatest common divisor we get that $(a, b) > 0$. By (ii) part of the definition of the greatest common divisor we get that $d|(a, b)$, so $(a, b) = d \cdot n$ for some $n \geq 1$ (since (a, b) and d are larger than zero). If $n > 1$ then $(a, b) > d$ impossible as d is the largest common divisor of a and b. Therefore $n = 1$ so $(a, b) = d$.

(Extended) Euclidean algorithm

- Let $a, b \in \mathbb{Z}$ be such that $a \geq b > 0$. Then by the division algorithm there exist (unique) integers q_1, r_1 such that $a = q_1 b + r_1$, $0 \leq r_1 < b$.

- Assuming that $r_1 > 0$, then we can apply the division algorithm to the pair b, r_1 and get $b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$. If $r_2 > 0$ then we may divide r_1 by r_2, and so on. We obtain a system of equations

  $$r_1 = q_3 r_2 + r_3$$

  ,

  $$0 \leq r_3 < r_2, r_2 = q_4 r_3 + r_4,$$

  where $0 \leq r_4 < r_3 3$.

- Continuing in this way, we get

  $$r_k = q_{k+2} r_{k+1} + r_{k+2}$$

  Notice that the terms in the sequence $b > r_1 > r_2 > ...$ are finite, strictly decreasing and non-negative, hence must eventually be zero.

- We will show that the last non-zero remainder r_{k+1} is the gcd(a,b). **Claim**. $r_{k+1} = (a, b)$. This follows on repeated application of the following Lemma, which gives $(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_k, r_{k+1}) = r_{k+1}$.

- **Lemma.** Let a, b, q, r be integers such that $a = qb + r$. Prove that the set S of common divisors of a and b is equal to the set T of common divisors of b and r. Deduce that gcd(a,b) = gcd(b,r).

- **Proof**. Let $c \in S$, so that there exists integers e, f such that $a = ce$ and $b = cf$. Then $a - qb = ce - qcf = c(e - qf)$. Thus c is a common divisor of both b and r; that is $c \in T$. Conversely, if $c \in T$, the same kind of argument shows that $c \in S$.

  Finally, gcd(a,b) is the largest positive member of S and gcd(b,r) is the largest positive member of T (see the exercise above). Since $S = T$ these numbers are the same.

Introduction to Number Theory

Agata Smoktunowicz

23th January 2019

Lecture 3

A note on authorship

These lecture notes include excerpts from notes written by Prof Tom Lenagan and Dr Mark Grant.

Plan for Lecture 3

1. Definition of primes, irreducibles, units.
2. Primes and irreducibles are the same in $\mathbb{Z}$.
3. Definition of Gaussian integers.

Things from previous lectures which we will need

Lemma. (Bezout) Let $a, b \in \mathbb{Z}$ (not both zero). If $d = gcd(a, b)$, then there exists $m, n \in \mathbb{Z}$ with $a \cdot m + b \cdot n = d$.

Factorisation in primes

We now move on to the subject of factorisation and primes in $\mathbb{Z}$.

Definition. Let $a, b, u \in \mathbb{Z}$.

(i) If $u|1$ then u is a **unit** in $\mathbb{Z}$.

(ii) If a is neither zero nor a unit, we say that a is **irreducible** in $\mathbb{Z}$ if whenever $a = cd$ for $c, d \in \mathbb{Z}$ it follows that either c or d is a unit.

(iii) If a is neither zero nor a unit, we say that a is **prime** in Z if whenever $a|cd$ with $c, d \in \mathbb{Z}$ it follows that $a|c$ or $a|d$.

Remarks.

- We allow negative primes (but discount 1 and -1 from being prime).

Exercise 1. The only units in $\mathbb{Z}$ are 1 and -1.

Proof. If $a > 1$ then $ab > 1$ for all $b > 0$ and $ab < 1$ for all $b < 0$. Similarly, if $a < -1$ then $ab < 1$ for all $b > 0$ and $ab > 1$ for all $b < 0$. Hence 1 and -1 are all units in $\mathbb{Z}$.

Exercise 2. If a is irreducible then $-a$ is also irreducible.

Proof. Assume that a is irreducible. If $-a = bc$ then $a = (-b)c$, and because a is irreducible, so either $-b$ or c is a unit, therefore either b or c is invertible. It follows that $-a$ is irreducible.

Lemma. Any integer a with $|a| > 1$ is a product of finitely many irreducibles.

Proof. We prove the result for all $a > 1$ - the result for $a < 1$ follows (by Exercise 2).

- Let S be the set of integers greater than 1 which cannot be written as a product of finitely many irreducibles. We wish to show $S = \emptyset$. So assume S is non-empty; by the well-ordering principle S has a least element, m say.

- This m cannot be irreducible (else we could write it as a product of one irreducible and it wouldnt be in S). It follows that $m = bc$ for some b, c with $1 < b,\ c < m$.

- Since m is the least element of S, neither b nor c are in S and hence both may be written as a product of finitely many irreducibles, $b = b_1b_2 \ldots b_k$ and $c = c_1c_2 \ldots c_j$. But then $m = b_1b_2 \ldots b_kc_1c_2 \ldots c_j$ may be written as a finite product of irreducibles, a contradiction. Hence $S = \emptyset$. (This is an example of a proof by minimum counter-example.)

Theorem 3. Let $a \in Z$ be neither zero nor a unit. Then a is prime if and only if a is irreducible.

Proof. $-- >$

- Let a be prime. We will show that a is irreducible. Suppose that $a = bc$. We need to show that either b or c is a unit. We can assume that $a, b, c > 0$ as other cases are done in a similar way.

- Since a is prime, then either $a|b$ or $a|c$.

- If $a|b$ then either $a = b$ or $a < b$ which is impossible as $a = bc$, it follows that $c = 1$. Similarly, if $a|c$ then $a = c$ and $b = 1$. Therefore either $b = 1$ or $c = 1$. It follows that a is irreducible.

$< --$

- Let a be irreducible. We will show that a is prime. Suppose that $a|bc$, we need to show that $a|b$ or $a|c$.

- If $a|b$ then we are done, so instead we assume that a does not divide b and aim to conclude that $a|c$.

- Since a is irreducible, its only divisors are $a, -a, 1, -1$. The only divisors it can have in common with b are therefore 1 and -1.

- It follows that $(a, b) = 1$, and that there exist $s, t \in Z$ with $sa + tb = 1$ (by the Bezout Lemma).

- Then $sac + tbc = c$. Clearly $a|sac$, and by our first assumption $a|bc$. Thus we find that $a|c$.

Gaussian integers

Definition. In this course a **ring** means a (not empty) subset of complex numbers which is closed under the addition, multiplication and subtraction. (in future years you will learn about other types of rings).

Define

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Then $\mathbb{Z}[i]$ is closed under the addition, multiplication and subtraction and therefore is a ring.

Introduction to Number Theory

Agata Smoktunowicz

25th January 2019

Lecture 4

A note on authorship

These lecture notes include excerpts from notes written by Prof Tom Lenagan and Dr Mark Grant.

Plan of Lecture 4

1. Gaussian integers. Units in Gaussian integers.
2. Prime and irreducible Gaussian integers.
3. Primes are exactly irreducibles in Gaussian integers (Theorem 4).
4. Every prime of the form $4k+1$ is a sum of two squares.

Gaussian integers

Definition. In this course a **ring** means a (not empty) subset the complex numbers which is closed under the addition, multiplication and subtraction.

Define
$$\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}.$$

Then $\mathbb{Z}[i]$ is closed under the addition, multiplication and subtraction and therefore is a ring (a tutorial exercise).

Let $z = a+ib$ be a Gaussian integer, then as usual we denote $|z| = |a+bi| = \sqrt{a^2+b^2}$ (where $a, b \in \mathbb{Z}$ and $i = \sqrt{-1}$).

Definition. (definition of a unit in $\mathbb{Z}[i]$). Similarly as before we say that a Gaussian integer $z = a+bi$ is a **unit** if there is a Gaussian integer $z' = a' + ib'$ such that $z \cdot z' = 1$.

Remark. If c, c' are Gaussian integers then $|c \cdot c'| = |c| \cdot |c'|$.
This is also true for arbitrary complex numbers c, c'.

Lemma 1. Let $z = a + ib$ be a unit in $\mathbb{Z}[i]$, then $|z| = 1$. Moreover, one of the following possibilities hold:

- $z = 1$

- $z = -1$
- $z = i$
- $z = -i$

(where $a, b \in \mathbb{Z}$).

Proof. If z is a unit in $\mathbb{Z}[i]$ then $z \cdot z' = 1$, so $|z| \cdot |z'| = 1$. Notice that for any Gaussian integer z we have $|z| \geq 1$ (why?). So $z \cdot z' = 1$ implies that $|z| = |z'| = 1$. Notice that $|z| = 1$ means $a^2 + b^2 = 1$, so either $a = 0$ or $b = 0$, as required. It follows that either $z = a$ or $z = ib$. Since $|z| = 1$ then $z \in \{-1, 1, i, -i\}$.

In Lecture 3 we proved that an integer is prime in $\mathbb{Z}$ if and only if it is irreducible in $\mathbb{Z}$.

What does it mean that a Gaussian integer is prime, or an irreducible?

Definition. Let z, z' be Gaussian integers. We say that $z \neq 0$ divides a Gaussian integer z', written as $z|z'$ if and only if $z' = z \cdot w$ for some Gaussian integer w.

Definition. Let $z = a + ib$ be a Gaussian integer (so $a, b \in \mathbb{Z}$) and z is not zero and not a unit (so $z \notin \{1, -1, i, -i, 0\}$). We say that z is an **irreducible** Gaussian integer if whenever $z = u \cdot v$ for Gaussian integers u, v it follows that either u or v is a unit, so either $u \in \{1, -1, i, -i\}$ or $v \in \{-1, 1, i, -i\}$.

Example 1. 2 is irreducible as an integer but 2 is not irreducible as a Gaussian integer, because $2 = (1 + i)(1 - i)$ and $1 + i, 1 - i$ are not units in Gaussian integers. So 2 is irreducible in $\mathbb{Z}$ but 2 is not irreducible in $\mathbb{Z}[i]$.

Example 2. 7 is irreducible as a Gaussian integer.

Proof. Suppose on the contrary that 7 is not irreducible as a Gaussian integer. Then, $7 = (a + ib)(c + id)$ for some $a, b, c, d \in \mathbb{Z}$ and $a + ib, c + id$ are not units. $7 = |(a + ib)(c + id)| = \sqrt{a^2 + b^2}\sqrt{c^2 + d^2}$. It follows that $49 = (a^2 + b^2)(c^2 + d^2)$.

Since 7 is a prime integer 7 divides either $a^2 + b^2$ or $c^2 + d^2$, hence either $7 = a^2 + b^2$ or $7 = c^2 + d^2$ (because by Lemma 1 we have $a^2 + b^2 \neq 1$ and $c^2 + d^2 \neq 1$.) It follows that 7 is a sum of two squares, which is impossible.

Definition. Let $z = a + ib$ be a Gaussian integer (so $a, b \in \mathbb{Z}$) and z is not zero and not a unit (so $z \notin \{1, -1, i, -i, 0\}$). We say that z is a **prime** Gaussian integer if whenever $z|u \cdot v$ for Gaussian integers u, v it follows that either $z|u$ or $z|v$.

We will take for granted the following theorem:

Theorem 4. Let $z = a + bi$ be a Gaussian integer, then z is a **prime Gaussian integer** if and only if z is an **irreducible Gaussian integer.**

A sketch of a proof for Theorem 4 for enthusiasts (not examinable):

It can be proved that a **Division algorithm holds** for Gaussian integers, namely:

Division algorithm. Let $a, b \in \mathbb{Z}[i]$ with $b \neq 0$, there exists $q, r \in \mathbb{Z}[i]$ with

$$a = qb + r$$

and either $r = 0$ or $|r| < |b|$.

Then we can use exactly the same proof as for integers (Lecture 3) when we proved that an integer is an irreducible integer if and only if it is a prime integer (instead of argument $a < b$ we need to use $|a| < |b|$).

Remark. For the exam you need to know Theorem 4 but you don't need to know a proof of it.

Corollary. 2 is not a prime Gaussian integer. 7 is a prime Gaussian integer.

Proof. Follows from Examples $1, 2$ and Theorem 4.

Which integers can be written as a sum of two squares?

The following theorem was stated but not proved by Fermat in the 1600s. Euler gave a proof in the 1700s.

Theorem Let $p = 4k + 1$ be a prime in $\mathbb{Z}$ for some integer $k > 0$. Then $p = a^2 + b^2$ for suitable $a, b \in \mathbb{Z}$.

Proof. (following Allenby in Rings, fields and groups) Suppose that $p = 4k + 1$ is a positive prime. Then p divides $1 + x^2$ where $x = (\frac{p-1}{2})!$ (see the next Lemma). Thus p divides $(1 + ix)(1 - ix)$ in $\mathbb{Z}[i]$. As p does not divide $1 + ix$ and p does not divide $1 - ix$, so p is not prime in $Z[i]$. As p is not prime it follows it is not irreducible in $Z[i]$. Thus we can write $p = (a + ib)(c + id)$, for suitable non-units $a + ib$, $c + id$ in $\mathbb{Z}[i]$. It follows that $p^2 = (a^2 + b^2)(c^2 + d^2)$. Since $a + bi$, $c + di$ are not units $a^2 + b^2 = p$, hence $p = (a + ib)(a - ib)$, as required.

Introduction to Number Theory

Agata Smoktunowicz

29th January 2019

Lecture 5

Plan of Lecture 5

1. Wilson's theorem.
2. If a number is a product of primes of the form $p = 4k + 1$ and squares of primes of the form $4k + 3$ then this number is a sum of two squares of integers.

Facts we will use:

We will use the following Theorem from Lecture 4. This theorem was stated but not proved by Fermat then later proved by Euler.

Theorem 4. Let $p = 4k+1$ be a prime in $\mathbb{Z}$ for some integer $k > 0$. Then $p = a^2 + b^2$ for suitable $a, b \in \mathbb{Z}$.

Remark. Observe that

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

This suggests that the problem of writing integers as sums of two squares may be reduced to the problem of deciding which primes can be written as sums of two squares. Therefore we get the following result:

Theorem 5. Let m, n be integers. If $m = x^2 + y^2$ and $n = u^2 + v^2$ for some $x, y, u, v \in \mathbb{Z}$, then $mn = z^2 + t^2$ for some integers z, t.

Theorem. Let $n = \prod_{i=1}^{m} p_i^{\alpha_i}$, where p_i are prime numbers and α_i are positive integers. Assume that whenever $p_i = 4k + 3$ then α_i is even (where $k \in \mathbb{Z}$). Then $p_i = x^2 + y^2$ for some integers x, y.

Proof. Follows from Theorems 4 and 5. Indeed, by Theorem 4 if $p_i = 4k+1$ for some $\in \mathbb{Z}$ then $p_i = x^2 + y^2$ for some integers x, y. By Theorem 5 applied several times we get that $p_i^{\alpha_i} = (x^2 + y^2)^{\alpha_i} = z_i^2 + t_i^2$ for some integers z_i, t_i. Similarly $2 = 1^2 + 1^2$ and, by Theorem 5 applied several times, we get that $2^m = (1^2 + 1^2)^m = z^2 + t^2$ for some integers z, t.

If $p_i = 4k + 3$ then $\alpha_i = 2k_i$ for some integer k_i so $p_i^{\alpha_i} = (p_i^{k_i})^2 + 0^2$. The result now follows from Theorem 5 applied several times. Later we will also prove that other integers cannot be written as a sum of squares.

Theorem 6. (Wilson's Theorem). For every prime number p, p divides $(p-1)! + 1$.

Proof.

1. We can list all integers modulo p as $\bar{0}, \bar{1}, \bar{2}, \dots, p \bar{-} 1$. Let X denote the set of all integers modul p which are not zero, so $X = \{\bar{1}, \bar{2}, \dots, p \bar{-} 1\}$.
2. We claim that for every $x \in X$ there is exactly one $y \in X$ such that $x \cdot y = \bar{1}$.
3. Indeed, if we fix $x \in X$ then we can consider all products $x \cdot \bar{1}, x \cdot \bar{2}, \dots, x \cdot \bar{p} - 1$, and observe that they all $\neq \bar{0}$ (because the product of two numbers not divisible by p is not divisible by p since p is prime).
4. It follows that all elements $x \cdot \bar{1}, x \cdot \bar{2}, \dots, x \cdot, p \bar{-} 1$ are distinct, as if $x \cdot \bar{i} = x \cdot \bar{j}$ for $p, q \in X$ then $x \cdot (i \bar{-} j) = \bar{0}$, a contradition with the above point 3. Therefore we can obtain every element from X as a product of x by some other element.
5. Therefore, for some element $y \in X$ we have $x \cdot y = \bar{1}$.
6. Notice that if $x = \bar{1}$ then $y = \bar{1}$ and if $x = \bar{-}1$ then $y = \bar{-}1$. However if $x \neq \bar{1}$ and $x \neq \bar{-}1$ then $x \neq y$ because otherwise $x^2 = \bar{1}$, so $(x - \bar{1})(x + \bar{1}) = 0$. This by 3 implies that either $x - \bar{1} = \bar{0}$ or $x + \bar{1} = \bar{0}$.
7. Therefore we can pair elements with their inverses, and we have $(p-3)/2$ such pairs. We also have elements $\bar{1}$ and $\bar{-}1$.
8. Hence we can multiply all different pairs and the product is one, and if we also multiply by 1 and -1 we get that $\bar{1} \cdots p \bar{-} 1 + \bar{1} = \bar{1} \cdot \bar{1} \cdots \bar{1} \cdot \bar{-}1 + \bar{1} = \bar{0}$, as required.

Corollary. Let p be a prime number and $p = 4k + 1$ for some integer k. Then p divides $((\frac{p-1}{2})!)^2 + 1$.

Proof. Note that $4k = p + 1$, so

$$(p \bar{-} 1)! = \bar{1} \cdot \bar{2} \cdots p \bar{-} 1 = (\bar{1} \cdot \bar{2} \cdots \bar{2k})((2k \bar{+} 1) \cdot (2k \bar{+} 2) \cdots (p \bar{-} 1)) =$$
$$(\bar{1} \cdot \bar{2} \cdots \bar{2k})((p \bar{-} 2k) \cdots (p \bar{-} 1)) =$$
$$= (\bar{1} \cdot \bar{2} \cdots \bar{2k})((-\bar{2}k) \cdots (-\bar{1})) = (\bar{2k}!)^2.$$

Thus, $[(2k)!]^2 \mathbf{mod(p)} = (p-1)! \mathbf{mod(p)}$.

So, by using Wilson's Theorem, we get that p divides $(p-1)! + 1$ and so p divides $[(2k)!]^2 + 1$.

However, $2k = ((4k+1) - 1)/2 = (p-1)/2$, and so p divides $((p-1)/2)!^2 + 1$, as required.

Introduction to Number Theory

Agata Smoktunowicz

29th January 2019

Lecture 6

Relationship to other material

Lecture 6 is based on Chapter 4 pages 20-22 from the Notes.

Plan of Lecture 6

Solving equations $ax + by = c$ in integers, in particular:

1. What we already know.
2. Better ways to find x, y.
3. Finding all solutions.
4. Finding nonnegative solutions.

What we already know

Let $a, b, c \in \mathbb{Z}$ and $b \neq 0$. From Lectures 1 and 2 and Tutorial 1 we know the following:

- We know that equation
$$ax + by = (a, b)$$
has a solution in integers if and only if $gcd(a, b)$ divides c.
- We know how to calculate gcd (a, b) using the Euclidean Algorithm.
- We know how to calculate x, y using the Euclidean algorithm in ' the reverse order'.

Better ways to find x, y

- Let $a, b, c \in \mathbb{Z}$ and $b \neq 0$. We would like solve equation
$$ax + by = (a, b)$$
in integers x, y.

- We wish to find some x, y satisfying this equation. We first write two copies of the equation $a \cdot x + b \cdot y = c$ for $x = 1, y = 0$ and also for $x = 0, y = 1$:

$$a = a \cdot 1 + b \cdot 0$$

$$b = a \cdot 0 + b \cdot 1$$

- On the left hand side we will apply the Euclidean algorithm, and we will modify the right hand side accordingly. We will continue in this way until we obtain $gcd(a, b)$ on the left hand side.

Example. Solve equation $5x + 13y = 1$ in integers x, y.

Proof.

- $$13 = 13 \cdot 1 + 5 \cdot 0$$ $$5 = 13 \cdot 0 + 5 \cdot 1$$

- The first remainder in the Euclidean Algorithm is: $$3 = 13 - 5 \cdot 2 = (13 \cdot 1 + 5 \cdot 0) - 2 \cdot (13 \cdot 0 + 5 \cdot 1) = 13 - 5 \cdot 2.$$

- The second remainder in the Euclidean algorithm is: $$2 = 5 - 3 = (13 \cdot 0 + 5 \cdot 1) - (13 - 5 \cdot 2) = 13 \cdot (-1) + 5 \cdot 3.$$

- The next remainder in the Euclidean Algorithm is: $$1 = 3 - 2 = (13 - 5 \cdot 2) - (13 \cdot (-1) + 5 \cdot 3) = 13 \cdot 2 + 5 \cdot (-5).$$

- We have solution $x = 2, y = -5$.

Finding all solutions of the equation $ax + by = c$

We did Theorem 4.1 from the Notes with proof (page 20 in the Notes).

Finding all nonnegative solutions of the equation $ax + by = c$

To find all nonnegative solutions we usually find all solutions (using Theorem 4.1 from the Notes) and then determine which of these solutions are nonnegative. We did Example 4.2 from the Notes to illustrate it (page 21 and 22 in the Notes).

Some closing remarks

Consider equation $ax + by = c$, where $b \neq 0$. If (a, b) does not divide c then we know that this equation has no solutions in integers.

Assume that (a, b) divides c, so $c/(a, b)$ is an integer. To find one solution to equation $ax + by = c$ it suffices to find a solution to $ax + by = (a, b)$ and then multiply it by $c/(a, b)$.

Usually, there are some integer solutions to equation $ax + by = c$ which cannot be obtained by multiplying a solution to $ax + by = (a, b)$ by $c/(a, b)$ (why?).

Introduction to Number Theory

Agata Smoktunowicz

5th February 2019

Lecture 7

Relationship to other material

Lecture 7 is partly based on pages 22 and 23 of the Notes (Chapter 4 section 1).

Plan of Lecture 7

1. Solving equations $a_1x_1 + \cdots + a_nx_n = c$ in integers using Euler's method.
2. Solving equations $a_1x_1+\cdots+a_nx_n = c$ in integers using the method from the Notes.
3. The Fundamental Theorem of Arithmetic.

A linear diophantine equation is an equation of the form

$$a_1x_1 + \ldots + a_nx_n = b$$

where $a_1, \ldots, a_n, b \in \mathbb{Z}$ and $a_k \neq 0$, for some $k \leq n$. Equations of this form have a solution if and only if the greatest common divisor of numbers $a_1, \ldots, a_n$ divides b, which we write as $(a_1, \ldots, a_n)|b$.

Example. The equation $6x_1 + 8x_2 + 12x_3 = 11$ has no integer solution as the LHS is even while the RHS is odd.

An important easy case. Let $a_1 = 1$. Then $x_2, x_3, \ldots, x_n$ can be chosen to be **any** integers, with our equation then determining x_1. Clearly this gives **all** of the solutions in this case.

We will look at two (very similar) methods in the context of solving a problem from 'Number theory in exercises' by Jerzy Rudkowski, namely solving in integers

$$7x + 8y + 10z = -99.$$

During the exam it does not matter which method(s) you use as long as you find all the solutions.

Euler's method

- We find the smallest coefficient: it is 7.
- We divide the equation by 7 to obtain the equation $(7x + 8x + 10z)/7 = -99/7$.
- We simplify the new equation so that one side is zero. We get $x+y+z+14+((y+3z+1)/7) = 0$.
- This equation has a solution if $y + 3z + 1 = 7t$ for some integer t.
- Our next step is to solve the equation $y+3z+1 = 7t$ in integers. This is equivalent to the equation $y + 3z - 7t + 1 = 0$.
- We use the same method to solve this equation. Out smallest coefficient is 1, so we can just write this equation as
$$y = 7t - 3z - 1.$$
- In conclusion we get $y = 7t-3z-1$, and consequently this implies $(y+3z+1)/7 = t$ hence $x+y+z+14+((y+3z+1)/7) = 0$ is equivalent to $x = -(y+z+14+t) = -(7t - 3z - 1 + z + 14 + t)$, hence $x = -8t + 2z - 13$.
- So the solution is
$$y = 7t - 3z - 1, x = -8t + 2z - 13, z = z$$
for integers t, z.

Method from the Notes

The general approach is to take linear changes of variables to successively reduce the minimum modulus of coefficients of our equation. We keep doing this until either

- $\gcd(a_1, a_2, \ldots, a_n) \neq b$, so no solution;
- we get a coefficient $= 1$, so we can solve as per the **easy case**.

We will now solve $7x + 8y + 10z = 99$ for integers x, y, z using this approach.

- Write the equation as $7x+8y+10z = 99$ and put $u = x+y$. So $7x+8y+10z = 99$ means
$$7u + y + 10z = 99,$$
where $x = u - y$. So
$$y = 99 - 10z - 7u.$$
- Now choose u, z arbitrarily in $\mathbb{Z}$. Then $y = 99 - 7u - 10z$ and $x = u - y = 8u + 10z - 99$.
- Thus the general solution is $(x, y, z) = (8u + 10z - 99, 99 - 7u - 10z, z)$.

The second solution algorithm in detail:

1. Pick the a_i of smallest modulus. If $|a_i| = 1$ we can solve our equation as per the **easy case** above.

2. Otherwise the smallest modulus of a_i is ≥ 2: For convenience, we assume that $a_1 > 0$ and a_1 has the smallest modulus among the a_i.

   (a) If all the a_i are divisible by a_1 and $a_1 \nmid b$ there is no solution.

   (b) If all the a_i are divisible by a_1 and $a_1 \mid b$ simply divide the equation by a_1. Now the new a_1 is $= 1$ so we can solve it by 1 above.

   (c) Otherwise choose an a_j **not** divisible by a_1 – assume it is a_2. Write $a_2 = qa_1 + a_2'$, where $0 < a_2' < a_1$, and put $u = x_1 + qx_2$. Then our equation becomes

   $$a_1x_1 + (qa_1 + a_2')x_2 + a_3x_3 \cdots + a_nx_n = b,$$

   or

   $$a_1u_1 + a_2'x_2 + a_3x_3 \cdots + a_nx_n = b. \tag{1}$$

   This new equation (1) has smallest coefficient $a_2' < a_1$. So we can repeat the process. We continue in this way until we get either (b) (there is a solution) or (a) (in this case there is no solution).

The Fundamental Theorem of Arithmetic

Fact 1. We will take for granted that if $a \cdot b = 0$ for $a, b \in \mathbb{Z}$ then either $a = 0$ or $b = 0$. Therefore, if $p, q, r \in \mathbb{Z}$ and $r \neq 0$ then $pr = qr$ implies $p = q$.

We will also use the following two results from Lecture 3:

Theorem 3. Let $a \in Z$ be neither zero nor a unit. Then a is prime if and only if a is irreducible.

Lemma. Any integer a with $|a| > 1$ is a product of finitely many irreducibles.

We can then prove the Fundamental Theorem of Arithmetic (the uniqueness of factorisation in $\mathbb{Z}$) as follows.

Let a be a nonzero integer. Then either a is a unit, or a may be expressed uniquely as a product of a unit and finitely many positive primes (up to re-ordering of factors). In other words, if $a = u \cdot p_1 \cdots p_k = v \cdot q_1 \cdots q_t$ where u, v are units and the p_i, q_j are positive primes, then $u = v, r = s$ and we can pair off the p_i and q_j such that paired primes are equal.

Proof. Part 1. Notice that, by Theorem 3, a may be expressed uniquely as a product of finitely many irreducible integers, and by the above Lemma irreducible integers are prime. It follows then that a may be expressed as a product of finitely many prime integers. Since 1 and -1 are units in $\mathbb{Z}$, it follows that a may be expressed as a product of a unit and finitely many positive primes.

Part 2. (unique presentation) Let $a = u \cdot p_1 \cdots p_k = v \cdot q_1 \cdots q_t$. Notice that p_1 divides a, so p_1 divides $v \cdot q_1 \cdots q_t$. Therefore $p_1 | q_i$, for some i. But q_i is prime, and hence irreducible, so its only divisors are $1, -1, q_i$ and $-q_i$. It follows that $p_1 = q_i$. We can divide by p_1 and continue in a similar way with $\bar{a} = up_2 \cdots p_n = v \prod_{k \neq j} q_j$ (by Fact 1).

Exercise. Is $132 \cdot 71 \cdot 103 = 23 \cdot 19 \cdot 53 \cdot 71$? Proof. As 19 does not divide 71, and 19 does not divide 103, these numbers are not equal.

Introduction to Number Theory

Agata Smoktunowicz

8th February 2019

Lecture 8

Relationship to other material

Lecture 8 is related to pages 24-32 of the Notes, especially Chapter 6 pages 29-32. Also this lecture contains examples similar to examples in the book entitled Number Theory in Exercises by Jerzy Rudkowski, PWN.

Plan of Lecture 8

1. Solving systems of linear equations in integers.
2. The Chinese remained theorem.

Solving systems of linear equations in integers

How might we solve systems of linear equations in integers? One way is to use methods from linear algebra, as for example the row operations don't change the solutions. We will use row operations with integer coefficients only.

Example.

Solve the following system of linear equations in integers and in natural numbers.

$$3x + 8y + 11z = 62$$

$$2x + 4y + 5z = 33$$

Solution. Using the row operations with integer coefficients we can do $R_2 \to R_2 - R_1$ to get:

$$3x + 8y + 11z = 62$$

$$-x + -4y - 6z = -29$$

The next row operations are $R_1 \to R_1 + 3R_2$ and $R_2 \to -R_2$:

$$-4y - 7z = -25$$

$$-x + -4y - 6z = -29$$

We can then do row operations $R_1 \to -R_1$ and $R_2 \to R_2$ to get

$$4y + 7z = 25$$

$$x + 4y + 6z = 29$$

The next step is (as in linear algebra) is to solve the equation $4y + 7z = 25$ and then calculate $x = 29 - 4y - 6z$.

We solve $4y + 7z = 25$ and obtain solution $y = 50, z = -25$. The general solution is then

$$y = 7t + 50$$

$$z = -4t - 25$$

We calculate then that:

$$x = 29 - 4y - 6z = -21 - 4t.$$

To obtain solutions in natural numbers, we need to assure that $x \geq 0, y \geq 0, z \geq 0$. This is equivalent to

$$7t + 50 \geq 0, -4t - 25 \geq 0, -21 - 4t \geq 0.$$

This in turn is equivalent to

$$t \geq -50/7, t \leq -25/4, t \leq -21/4.$$

The only solution is $t = -7$. So the only natural numbers solution is $(x, y, z) = (7, 1, 3)$.

The Chinese remainder theorem

Let $m_1, m_2, \ldots, m_k$ be natural numbers such that the greatest common divisor of any two of them is 1. Let $a_1, a_2, \ldots, a_k$ be arbitrary integers. Then there is x such that:

$$x \equiv a_1 \mathbf{mod} m_1$$

$$x \equiv a_1 \mathbf{mod} m_2$$

$$\ldots$$

$$x \equiv a_k \mathbf{mod} m_k$$

This solution (x) is unique modulo $m_1 m_2 \cdots m_k$.

Proof.

1. Let $N = m_1 m_2 \cdots m_k$ and $N_i = N/m_i$, for every i.
2. Fix i. There exists a solution to the congruence
$$N_i x \equiv 1 \mathbf{mod} m_i$$
because this congruence is equivalent to the equation
$$N_i x + m_i y = 1$$
and the greatest common divisor of N_i and m_i is 1.
3. Let $x_i \in \mathbb{Z}$ be such that
$$N_i x_i \equiv 1 \mathbf{mod} m_i.$$
4. Denote $x = \sum_{i=1}^{k} a_i N_i x_i$. Then $x \equiv a_i \mathbf{mod} m_i$ for $i = 1, 2, \ldots, k$.
5. Observe that $x' = x + jN$ also satisfies $x \equiv a_i \mathbf{mod} m_i$ for $i = 1, 2, \ldots, k$.
6. Notice on the other hand that if x, x' are solutions to the above system of congruences then $x - x' \equiv 0 \mathbf{mod} m_i$ for each i, so $x - x' = jN$, for some integer j.

Exercise. Solve the following system of congruences.

$$x \equiv 1 \mathbf{mod} 2$$
$$x \equiv 3 \mathbf{mod} 5$$
$$x \equiv 4 \mathbf{mod} 7$$

Solution. We proceed as in the proof of the Chinese remainder theorem. We have $N = 2 \cdot 5 \cdot 7 = 70$, $N_1 = 70/2 = 35$, $N_2 = 70/5 = 14$, $N_3 = 70/7 = 10$.

We need to solve congruences

$$35 x_1 \equiv 1 \mathbf{mod} 2$$
$$14 x_2 \equiv 1 \mathbf{mod} 5$$
$$10 x_3 \equiv 1 \mathbf{mod} 7$$

We can take $x_1 = 1$, $x_2 = 4, x_3 = 5$. Consequently, we can take $x = a_1 x_1 N_1 + a_2 x_2 N_2 + a_3 x_3 N_3 = 1 \cdot 1 \cdot 35 + 3 \cdot 4 \cdot 14 + 4 \cdot 5 \cdot 10 = 35 + 168 + 200 = 403$. Notice that $x = 53$ is also a solution, since $53 = 403 - 70 \cdot 5$.

Introduduction to Number Theory

Agata Smoktunowicz

12th February 2019

Lecture 9

Plan of Lecture 9

- Systems of congruences which don't fit the Chinese remainder theorem context.
- Fermat's Little theorem, primitive roots.

Systems of congruences

Let a_i, m_i be integers ($m_i \neq 0$). Consider systems of congruences

$$\begin{gathered} x \equiv a_1 (\mod m_1) \\ x \equiv a_2 (\mod m_2) \\ \dots \\ x \equiv a_k (\mod m_k) \end{gathered}$$

What happens if numbers m_i, m_j are not coprime for some i, j?

Main fact to use. Let m, n be two integers such that the greatest common divisor of m, n is 1. Let $a \in \mathbb{Z}$, then the congruence

$$x \equiv a (\mod m \cdot n)$$

has the same solutions in integers as the following system of congruences

$$\begin{gathered} x \equiv a (\mod m) \\ x \equiv a (\mod n) \end{gathered}$$

Proof. If $x \equiv a(\mod m \cdot n)$ then clearly $x \equiv a(\mod m)$ and $x \equiv a(\mod n)$. On the other hand, if $x \equiv a(\mod m)$ and $x \equiv a(\mod n)$ then $x - a = k \cdot m$ and $x - a = k' \cdot n$ so n divides k (where k, k' are some integers). It follows that $x - a \equiv 0($ mod $m \cdot n)$, so $x \equiv a(\mod m \cdot n)$.

Conclusion. Knowing a number $x \mod N$ is equivalent to knowing $x \mod$ each of the prime powers $p_j^{e_j}$ in $N = p_1^{e_1} \cdots p_n^{e_n}$. For example, knowing that $x \equiv 27 (\mod 30)$ is the same as knowing $x \equiv 1 (\mod 2)$, $x \equiv 0 (\mod 3)$, $x \equiv 2 (\mod 5)$.

Exercise 1. Solve the system of congruences

$$x \equiv 19 (\mod 45)$$
$$x \equiv 21 (\mod 55)$$

Solution. By the above fact it is equivalent to solve

$$x \equiv 19 (\mod 5), x \equiv 19 (\mod 9)$$
$$x \equiv 21 (\mod 5), x \equiv 21 (\mod 11)$$

This system of congruences has no solutions as

$$x \equiv 19 (\mod 5) \equiv 4 (\mod 5)$$

and

$$x \equiv 21 (\mod 5) \equiv 1 (\mod 5)$$

are contradictory with each other.

Exercise 2. Solve the system of congruences

$$x \equiv 6 (\mod 200)$$
$$x \equiv 81 (\mod 375)$$

Solution. By the above fact it suffices to solve

$$x \equiv 6 (\mod 8), x \equiv 6 (\mod 25)$$
$$x \equiv 81 (\mod 125), x \equiv 81 (\mod 3)$$

Notice that if $x \equiv 81 (\mod 125)$ then $x \equiv 6 (\mod 25)$ so we only need to solve three congruences

$$x \equiv 6 (\mod 8),$$
$$x \equiv 81 (\mod 125),$$
$$x \equiv 81 (\mod 3) \equiv 0 (\mod 3)$$

We can now apply the Chinese remainder theorem method for $m_1 = 8, m_2 = 125, m_3 = 3$, $a_1 = 6$, $a_2 = 81$, $a_3 = 0$. We find $N = m_1 \cdot m_2 \cdot m_3 = 3000$, $N_1 = 375$, $N_2 = 24$, $N_3 = 1000$. We find solutions to congruences $375x_1 \equiv 1 (\mod 8)$ (which is equivalent to $7x_1 \equiv 1 (\mod 8)$), $24x_2 \equiv 1 (\mod 125)$, $1000x_3 \equiv 1 (\mod 3)$. We can take $x_1 = 7$, $x_2 = -26$, $x_3 = 1$ (to calculate x_2 we solved $24x + 125y = 1$).

A solution is $x \equiv 7 \cdot 6 \cdot 375 - 81 \cdot 26 \cdot 24 + 1 \cdot 0 \cdot 1000 (\mod 3000) \equiv 15,750 - 50,544 (\mod 3000) \equiv -34794 (\mod 3000) \equiv 1206 (\mod 3000)$.

Exercise. Find a solution of the congruence $24x \equiv 3 \mod 33$.

Proof. We can write this congruence as an equation

$$24x + 33y = 3,$$

then to get the solution we divide both sides by 3 to get

$$8x + 11y = 1.$$

We can solve it in the usual way:

$$8 \cdot 0 + 11 \cdot 1 = 11,$$

$$8 \cdot 1 + 11 \cdot 0 = 8,$$
$$8 \cdot (-1) + 11 \cdot 1 = 3,$$
$$8 \cdot 1 - 2(8 \cdot (-1) + 11 \cdot 1) = 2,$$
$$8 \cdot 3 - 11 \cdot 2 = 2,$$
$$(8 \cdot (-1) + 11 \cdot 1) - (8 \cdot 3 - 11 \cdot 2) = 3 - 2 = 1,$$
$$8 \cdot (-4) + 11 \cdot 3 = 1,$$

Hence $x = -4$ is a solution, as well as $x = -4 + 11 = 7$. Notice that every solution x is of the form $x \equiv 7(\mod 11)$ which means that $x = 7 + k \cdot 33$ for $k \in \mathbb{Z}$. Notice that $24 \cdot x = 24 \cdot 7 \equiv 3 \mod 11$.

Exercise. Let $m, n \in \mathbb{Z}$ be such that the $gcd(m, n) = 1$. Show that there is $q \in \mathbb{Z}$ such that

$$mq \equiv 1 \mod n.$$

Proof. By Bezout lemma the equation

$$mx + ny = 1$$

has a solution x. We can take it that $q = x$, then $mq = mx = 1 - ny \equiv 1 \mod n$.

Fermat's Little Theorem

Let p be a prime number, and let a be any number with $a \neq 0 \mod p$. Then

$$a^{p-1} - 1 \equiv 0(\mod p)$$

Proof. Consider elements

$$1(\mod p), 2(\mod p), \dots, p-1(\mod p).$$

We claim that the elements

$$a(\mod p), 2 \cdot a(\mod p), \dots, (p-1) \cdot a(\mod p)$$

are the same elements, in a possibly different order.

Observe that indeed all the elements $a(\mod p), 2 \cdot a(\mod p), \dots, (p-1) \cdot a(\mod p)$ are all pairwise distinct, and there are $p-1$ of them, so each element $i \mod p$ will appear in the second sequence, and exactly once.

Indeed, if $i \cdot a(\mod p) \equiv j \cdot a(\mod p)$ then $(i-j) \cdot a = 0(\mod p)$, so p divides $i - j$ so $i = j$.

Now the products of all elements in the mentioned two sentences will be the same (as they differ only by the order of elements). Therefore

$$1 \cdot 2 \cdot (p-1)(\mod p) \equiv a \cdot 2a \cdot 3a \cdot (p-1)a(\mod p).$$

It follows that $(p-1)! \equiv (p-1)!a^{p-1}(\mod p)$. By Wilson's theorem, $(p-1)! \equiv -1(\mod p)$, hence

$$-1 \equiv -a^{p-1}(\mod p).$$

Therefore $a^{p-1} - 1 \equiv 0(\mod p)$.

Primitive roots

During Workshop 3 for Honours Algebra it was shown that for every prime number p there is an integer $1 \leq \xi < p$ such that $\xi^{p-1} = 1(\mod p)$ and $\xi^n(\mod p) \neq 1(\mod p)$ for $1 \leq n < p - 1$.

Notice that it follows that all the elements $\xi, \xi^2, \dots, \xi^{p-1}$ give pairwise distinct remainders modulo p, therefore for every $0 < n \leq p$ there is $\alpha \leq p - 1$ such that

$$n \equiv \xi^{\alpha}(\mod p).$$

Exercise 1. Find the remainder $0 \leq r < 13$ from dividing 2^{100} by 13.

Proof. $100 = 4 + 12 \cdot 8$, hence $2^{100} \equiv 2^4 \cdot (2^{12})^8 \mod 13 = 2^4 \mod 13 = 3 \mod 13$.

Exercise 2. Let p be a prime number, and a be coprime with p. Find a solution of the congruence $ax \equiv 1 \mod p$.

Proof. By Fermat's Little theorem we have $x = a^{p-2}$ is a solution.

(Z_n, The ring of integers $\mod n$) Let n be a positive integer, and let $a, b, c \in \mathbb{Z}$. We say a is congruent to $b \mod n$ (written $a \equiv b(\mod n)$ or $a \equiv b \mod n$) if $n|(b-a)$. It is easily shown that

- (i) $a \equiv a(\mod n)$,
- (ii) $a \equiv b(\mod n)$ implies $b \equiv a(\mod n)$,
- (iii) $a \equiv b(\mod n)$ and $b \equiv c(\mod n)$ implies $a \equiv c(\mod n)$.

Hence congruence $\mod n$ defines an equivalence relation on $\mathbb{Z}$. Let Z_n denote the set of equivalence classes, and denote the equivalence class of $a \in \mathbb{Z}$ by $[a]_n \in \mathbb{Z}_n$ Observe that

$$[r]_n = \{r + kn : k \in \mathbb{Z}\}.$$

By the division algorithm there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $a = qn + r$. Hence $n|a - r$ and $[a]_n = [r]_n$, so the equivalence class of a is determined by its remainder on division by n (sometimes called its residue mod n). Hence $\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n-1]_n\}$ has exactly n elements. Elements $[i]_n$ are called co-sets, as $[r]_n$ is called a co-set of r). You check that the addition and multiplication on $\mathbb{Z}_n$ defined by

$$[a]_n + [b]_n = [a+b]_n, [a]_n \cdot [b]_n = [ab]_n$$

are well-defined (this means the definition doesnt depend upon the choice of representative for each class; you will have to check, for example, that if $a \equiv c(\mod n)$ and $b \equiv d(\mod n)$ then $a + b \equiv c + d(\mod n)$. With these operations so defined, $\mathbb{Z}_n$ becomes a commutative ring with identity.

A question from the audience was: "What is $a(\mod p)$, a set, or an element?

Answer. It is both a set and an element (in this lecture). The reason for this question is perhaps that I used a slight abuse of the notation with regard to what $a(\mod n)$ means in the proof of Fermat's Little theorem. Here is what I meant:

In the proof of Fermat's Little theorem, by a slight abuse of notation, I denoted $[r]_n$ by $r(\mod n)$ (where $[r]_n$ is an element of Z_n as above). Therefore, r_n and $r(\mod n)$ in this lecture mean an element of $\mathbb{Z}_n$ (and a co-set of r). Recall that,

$$[r]_n = \{r + kn : k \in \mathbb{Z}\}.$$

We also denote $\mathbb{Z}_n$ as $\mathbb{Z}/n\mathbb{Z}$ (so they mean the same thing).

Introduction to Number Theory

Agata Smoktunowicz

15th February 2019

Lecture 10

Plan of Lecture 10

- The Legendre symbol. Main facts.
- The Legendre symbol. Typical exercises.
- Primitive roots.
- A comment on congruences.

The Legendre symbol

Let $p > 0$ be a prime number and let $a \in \mathbb{Z}$ be an integer not divisible by p.

- The Legendre symbol of a modulo p is $(\frac{a}{p})$.
- It is 1 if $a \equiv r^2(\mod p)$ for some integer r and -1 otherwise.
- If $(\frac{a}{p}) = 1$ then we say that a is a quadratic residue modulo p.

Facts we will use to solve Legendre symbol exercises:

Theorem 7

Let $p > 0$ be a prime number and let $a \in \mathbb{Z}$ be an integer not divisible by p. Then the following hold:

1. Let p be an odd prime number. The formula for the Legendre symbol is

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}(\mod p).$$

2. Quadratic residue multiplication rule

$$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$$

3. $$(\frac{a}{p}) = (\frac{a-p}{p}).$$

   Moreover if $a \equiv b(\mod p)$ then

   $$(\frac{a}{p}) = (\frac{b}{p}).$$

4. Quadratic reciprocity, part 1: Let $p, q > 0$ be distinct odd primes, then

   $$(\frac{p}{q}) = (\frac{q}{p})$$

   provided that either $p \equiv 1(\mod 4)$ or $q \equiv 1(\mod 4)$.

5. Quadratic reciprocity, part 2: Let $p, q > 0$ be distinct odd primes, then

   $$(\frac{p}{q}) = -(\frac{q}{p})$$

   provided that $p \equiv 3(\mod 4)$ and $q \equiv 3(\mod 4)$.

Proofs.

1. If $a = r^2(\mod p)$ then $a^{\frac{p-1}{2}} = r^{p-1} = 1(\mod p)$ by Fermat's Little theorem.

   Suppose that $a^{\frac{p-1}{2}} \equiv 1(\mod p)$. Let ξ be a primitive root. Then $a = \xi^\alpha$ for some α, since ξ is a primitive root. Now $a^{\frac{p-1}{2}} \equiv 1(\mod p)$ implies $\xi^{\alpha \cdot \frac{p-1}{2}} = 1$. Since ξ is a primitive root this implies that $p-1$ divides $\alpha \cdot \frac{p-1}{2}$, hence α is even. Let $r = \xi^{\alpha/2}$, then $a \equiv r^2(\mod p)$.

2. Follows from (1).

3. Since we are considering congruences modulo p adding or subtracting p does not affect the result.

4. Will be proved later (difficult).

5. Will be proved later (difficult).

Questions on quadratic residues

Exercise 1. Show that

- $(\frac{-1}{p}) = 1$ provided that $p \equiv 1(\mod 4)$ and
- $(\frac{-1}{p}) = -1$ provided that $p \equiv 3(\mod 4)$

Proof. Follows from Theorem 7 (1), since $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} (\mod p)$.

Exercise 2. Calculate $(\frac{2}{7})$.

Solution. By Theorem 7 (1) we have $(\frac{2}{7}) \equiv 2^{\frac{7-1}{2}} (\mod 7) \equiv 8 (\mod 7) \equiv 1 (\mod 7)$. It follows that $(\frac{2}{7}) = 1$.

Another solution: By Theorem 7 (3) we have $(\frac{2}{7}) = (\frac{9}{7})$. By Theorem 7 (2) we have $(\frac{9}{7}) = (\frac{3}{7}) \cdot (\frac{3}{7}) = 1$.

(Notice that we could not use Theorem 7 (4) and (5) as they are only for odd numbers).

Exercise 3. Calculate $(\frac{7}{13})$.

Proof 1.

1. Notice that $13 = 1 (\mod 4)$. Therefore by Theorem 7, (4) we get that $(\frac{7}{13}) = (\frac{13}{7})$.
2. By Theorem 7, (3) we get $(\frac{13}{7}) = (\frac{6}{7})$.
3. By Theorem 7, (2) we get
   $(\frac{6}{7}) = (\frac{2}{7}) \cdot (\frac{3}{7})$.
4. By Exercise 2, $(\frac{2}{7}) = 1$.
5. By Theorem 7, (5) we get $(\frac{3}{7}) = -(\frac{7}{3})$
6. By Theorem 7, (3) we get $(\frac{7}{3}) = (\frac{1}{3})$.
7. Consequently, $(\frac{7}{13}) = -1$, so 7 is not a quadratic residue modulo 13.

Proof 2. (Suggested by a student during the lecture)

1. Notice that $13 = 1 (\mod 4)$. Therefore by Theorem 4, (4) we get that $(\frac{7}{13}) = (\frac{13}{7})$.
2. By Theorem 7, (3) we get $(\frac{13}{7}) = (\frac{-1}{7})$.
3. By Exercise 1 we get $(\frac{-1}{7}) = -1$.
4. Therefore $(\frac{7}{13}) = -1$.

Primitive roots and a lemma we used in the proof of Theorem 7, (1)

Definition. Let p be a prime number. Let ξ be an integer not divisible by p, then ξ is a primitive root if and only if $\xi^i (\mod p) \neq 1 (\mod p)$ for $1 \leq i < p - 1$.

Notice that by Fermat's Little theorem $\xi^{p-1} \equiv 1 (\mod p)$.

Recalling what we know from Honours Algebra:

Theorem 8. $\mathbb{Z}_p$ is a field. For every prime number p the field $\mathbb{Z}_p$ has a primitive root.

Proof. It was proved during Workshop 3 from Honours Algebra.

Lemma. Let $a, i, j \in \mathbb{Z}$, p be prime and suppose that a is not divisible by p. Suppose that $a^i \equiv 1(\mod p)$ and $a^j \equiv 1(\mod p)$. Show that $a^{(i,j)} \equiv 1(\mod p)$.

Proof. By Theorem 2 (from Lectures 1 and 2) there are $\alpha, \beta \in \mathbb{Z}$ such that $i\cdot\alpha + j\cdot\beta = (i, j)$. Observe that

$$a^{(i,j)} = a^{i\cdot\alpha+j\cdot\beta} = (a^i)^\alpha \cdot (a^j)^\beta \equiv 1(\mod p).$$

A comment about congruences motivated by a student's e-mails, with some of his comments included.

If you are asked to 'solve a congruence' $ax \equiv b(\mod n)$ (for example $24x = 3(\mod 33)$) then we need to find solutions $x \in \mathbb{Z}$. So for example for the congruence

$$24x = 3(\mod 33)$$

if you write $x \equiv 7(\mod 11)$ then it means that $x = 7 + k \cdot 11$ for $k \in \mathbb{Z}$, so it is a good solution just to write $x \equiv 7(\mod 11)$.

Sometimes you may be asked to find all the solutions of type $x(\mod n)$ with $0 \leq x < n$, but it will always be mentioned in the question if we are being asked for solutions in this form. In our case the solutions would be $x \equiv 7(\mod 33)$, $x \equiv 18(\mod 11)$, $x \equiv 29(\mod 11)$.

Introduction to Number Theory

Agata Smoktunowicz

26th February 2019

Lecture 11

Plan of Lecture 11

- Euler's theorem.
- Euler's function.

Euler's function

Recall that for $n > 1$ the Euler function $\phi(n)$ is defined as the number of natural numbers not exceeding n which are coprime with n, and for $n = 1$ we have $\phi(1) = 1$.

Euler's theorem

Let $n > 1$ be a natural number, and let a be any number such that the greatest common divisor of a and n is 1 (in other words n and a are coprime). Then

$$a^{\phi(n)} - 1 \equiv 0(\mod n)$$

Proof. Let $1 \leq k_1, k_2, \ldots, k_{\phi(n)} < n$ be all numbers coprime with n. We can list elements

$$k_1(\mod n), k_2(\mod n), \ldots, k_{\phi(n)}(\mod n).$$

We claim that the numbers

$$k_1 \cdot a(\mod n), k_2 \cdot a(\mod n), \ldots, k_{\phi(n)} \cdot a(\mod n)$$

are the same elements, in a possibly different order. Notice that all these elements are coprime with n, and each two of them are pairwise distinct (by the same argument as in Fermat's Little theorem). Therefore the products of all elements in each of these two sentences are equal. It follows that

$$k_1 \cdot k_2 \cdots k_{\phi(n)} = k_1 \cdot k_2 \cdots k_{\phi(n)}(\mod n) = k_1 \cdot k_2 \cdots k_{\phi(n)} a^{\phi(n)}(\mod n)$$

Since $q = k_1 \cdot k_2 \cdots k_{\phi(n)}$ is coprime with n, then there is q' such that $qq' = 1 \mod n$, so we can multiply the above equation by q' and get

$$1 \equiv a^{\phi(n)}(\mod n).$$

For the following theorem and exercise I used excerpts from the book "Number theory" by Marek Zakrzewski, PWN.

Theorem. If m, n are coprime then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Proof. Consider the matrix

$$\begin{bmatrix} 1 & 2 & \cdots & m \\ m+1 & m+2 & \cdots & 2m \\ \vdots & \vdots & \ddots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & nm \end{bmatrix}$$

Observe that in each column of this matrix the elements give the same remainder modulo m. Therefore either all are coprime with m or all are not coprime with m. The number of columns which are coprime with m is $\phi(m)$. In each of these columns the elements give all possible remainders modulo n. Therefore each column has $\phi(n)$ elements coprime with n. Therefore the number of elements smaller than mn which are coprime with $m \cdot n$ is $\phi(m)\phi(n)$.

Exercise 3. Suppose that $p(1), \ldots, p(j)$ are distinct primes that divide m. Show that the following formula is correct

$$\phi(m) = m(1 - \frac{1}{p(1)})(1 - \frac{1}{p(2)}) \ldots (1 - \frac{1}{p(j)}).$$

Use this formula to compute $\phi(120)$.

Proof. It suffices to show that for a prime number p, $\phi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$. This follows as to calculate numbers smaller than p^n which are coprime with p^n it suffices to calculate numbers smaller than p^n which are coprime with p.

We calculate $120 = 8 \cdot 5 \cdot 3$, hence $\phi(120) = (8-4)(5-1)(3-1) = 32$.

Exercise. Let n be a number such that $a^{n-1} = 1 \mod n$ for every a coprime with n. Does it follow that n is prime?

Solution. No, for example $n = 561 = 3 \cdot 11 \cdot 17$.

A number n such that $a^{n-1} = 1 \mod n$ for every a coprime with n is called a Carmichael number.

Exercise. Let n be a number such that $a^{n-1} = 1 \mod n$ for every $0 < a < n$. Show that n is a prime number.

Proof. Suppose on the contrary, and let $1 < p$ be a divisor of n. Then $p^{n-1} \neq 1($ mod $n)$ since p divides n.

Exercise. Calculate $\phi(120)$.

Proof. $120 = 2^3 \cdot 5 \cdot 3$, therefore $\phi(120) = 4 \cdot 4 \cdot 2 = 32$.

Exercise. Find an integer n with $\phi(n) = 4$.

Proof. We will use the formula from Corollary 1. Let $n = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Notice that if p_i is odd then $\alpha_i = 1$ as otherwise α_i would divide $n = 4$, impossible. Observe that $p_1 - 1$ divides 4, so $p_1 - 1 \in \{1, 2, 4\}$, so $p_1 \in \{2, 3, 5\}$. If $p_1 = 5$, then $n = 5$ or $n = 10$. If $p_1 = 3$ then $n = 3 \cdot 4$, if $p_1 = 2$ then $n = 8$.

Introduction to Number Theory.

Agata Smoktunowicz

1st March 2019

Lecture 12

Plan for Lecture 12

- Existence of a primitive root in $\mathbb{Z}_p$ (p-prime).
- $\mathbb{Z}_p$ is cyclic.
- Exercises on Euler function $\phi(n)$.

I have uploaded the lecture notes from Number Theory from the year 2014 by Adam Boocher (University of Edinburgh). These notes are very well organized and well presented. During Lecture 12 we looked at:

- Theorem 10.1 from pages 36-37 from the Chapter 10.1 and
- Theorem 10.8 on page 37 from the Chapter 10.3 and
- Theorem 10.4 with their proofs (page 36 for the statement, and end of page 37 for the proof).

Exercise. Let $n > 1$ be an integer. Find all n with $\phi(n) = 2$.

Proof. We will use the formula for the Euler's function. Let $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ where $p_1, \dots, p_m > 1$ are pairwise distinct prime integers. We know the formula for $\phi(n)$:

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \dots (p_m^{\alpha_m} - p_m^{\alpha_m - 1}).$$

Notice first that $p_i - 1$ divides $\phi(n)$ for every i, so $p_i - 1$ equals either 2 or 1, so $p_i \in \{2, 3\}$.

Suppose that p has only one prime divisor then $n = p_1^{\alpha_1}$ so $\phi(n) = p_1^{\alpha_1} - p_1^{\alpha_1 - 1} = p_1^{\alpha_1 - 1}(p_1 - 1)$. Notice that if $p_1 = 2$ then $n = 4$, and if $p_1 = 3$ then $n = 3$.

We can assume now that n has more than one prime divisor, then $n = p_1^{\alpha_1} \dots p_2^{\alpha_2}$. Then $\phi(n) = (2^{\alpha_1} - 2^{\alpha_1 - 1})(3^{\alpha_2} - 3^{\alpha_2 - 1}) = 2^{\alpha_1 - 1} 3^{\alpha_2 - 1}(3 - 1)$ so $\alpha_1 - 1 = 0$ and $\alpha_2 - 1 = 0$, hence $n = 6$.

Introduction to Number Theory.

Agata Smoktunowicz

5th March 2019

Lecture 13

Plan of Lecture 13

- We did Exercise 1 from Tutorial 4 (the solution can be found in Tutorial 4).
- Strengthening Euler's theorem $a^{\phi(n)} \equiv 1(\mod n)$.
- For which natural number n there exist primitive roots in $\mathbb{Z}_n^*$.

Strengthening Euler's theorem

We define the least common multiple of integers $i_1, \ldots, i_n$ to be the smallest positive integer m such that $i_1|m$, $i_2|m$, $\ldots, i_n|m$. It will be denoted as $lcm(i_1, i_2, \ldots, i_n)$.

Theorem. Suppose that an integer n factorizes as

$$n = p_1^{f_1} \ldots p_k^{f_k}.$$

Let a be an integer such that $gcd(a, n) = 1$. Then

$$a^N = 1(\mod n),$$

where

$$N = lcm(p_1^{f_1} - p_1^{f_1 - 1}, p_2^{f_2} - p_2^{f_2 - 1}, \ldots, p_k^{f_k} - p_k^{f_k - 1}).$$

Proof. Let's first work modulo a prime power. Let $m = p^f$ where $p > 1$ is a prime number. Then we know that if $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \mod m$, i.e. $a^{p^f - p^{f-1}} = 1($ mod $m)$. Hence in the notation of the question, we see that

$$a^{p_i^{f_i} - p_i^{f_i - 1}} = 1(\mod p_i^{f_i}).$$

Hence, if N is the lcm of all of these exponents, then $a^N - 1$ will certainly be divisible by all the $p_i^{f_i}$ and thus it will be zero modulo n.

Exercise. For which n is this result no stronger than Euler's theorem $a^{\phi} \equiv 1($ mod $n)$? For which n is this result stronger than Euler's theorem?

Proof. By Corollary 2, we know that the formula for $\phi(n)$ is $(p_1^{f_1} - p_1^{f_1-1}) \cdots (p_k^{f_k} - p_k^{f_k-1})$.

Observations.

Observe that $\phi(n)$ will equal N iff all the $p_j^{f_j} - p_j^{f_j-1}$ are coprime. In particular 2 cannot divide both $p_i^{f_i} - p_i^{f_i-1}$ and $p_j^{f_j} - p_j^{f_j-1}$ for any $i \neq j$. We have the following cases:

1. Suppose that n has two distinct odd prime divisors, say p_1 and p_2, then $2|p_1-1$ and $2|p_2-1$ then $lcm(n) < \phi(n)$ (as a bigger power of 2 will divide $\phi(n)$ than $lcm(n)$) so in this case the above result is stronger than Euler's theorem.
2. If $n = p^{\alpha}$ for some prime number n then the above result is equivalent to Euler's theorem, so is no stronger.
3. If $n = 2p^{\alpha}$ for an odd prime p and $\alpha > 0$ then the result is not stronger.
4. If $n = 2^i p^{\alpha}$ for $i > 1, \alpha > 0$ then the above result is stronger the Euler's theorem.

Corollary 2. Let n be a prime number which is divisible by two distinct odd prime numbers, or by 4 and an odd prime number. Then there is number $0 < N < \phi(n)$ such that $a^N \equiv 1($ mod $)$ for every a coprime with m.

Primitive roots in $\mathbb{Z}_n^*$ for not prime n.

Let n be an integer. We will say that $a \in \mathbb{Z}$ is a primitive root for n, or more formally that $a \in \mathbb{Z}$ is a primitive root in $\mathbb{Z}_n^*$ if

$$a^{\phi(n)} \equiv 1 \mod n$$

and

$$a^i \mod n \neq 1 \mod n$$

for $0 < i \leq \phi(n)$.

Notice that the second congruence implies that $gcd(a, n) = 1$.

Theorem. A positive integer n has a primitive root if and only if n is one of the following numbers

$$2, 4, p^k, 2 \cdot p^k$$

where p is an odd prime and k is a positive integer.

Proof. The implication → follows from Corollary 2. We will not prove the implication in the other direction, but we will do some related exercises in Tutorial 4.

Introduction to Number Theory.

Agata Smoktunowicz

8th March 2019

Lecture 14

Plan of Lecture 14

- Gauss Lemma.
- An exercise to calculate the Legendre symbol $(\frac{a}{p})$.

Gauss Lemma

Let p be an odd prime number and a be an integer not divisible by p. Consider the set $S = \{a, 2 \cdot a, 3 \cdot a, \dots, \frac{p-1}{2} \cdot a\}$. Let S' be the set of remainders of elements from set S when divided by p, with each remainder larger than 0 and smaller than p. Then all elements of the set S' are larger than 0 and smaller than p. Let n denote the number of elements from set S' which are larger than $\frac{p}{2}$. Then

$$(\frac{a}{p}) = (-1)^n.$$

Proof. For proof see the proof of Lemma 16.2 from Adam Boocher's Number Theory notes from the 2014 course, pages 51 and 52, which is basically the same as the proof that we covered in the lectures. Please notice that $p - i \equiv -i \mod p$, so the statement of Lemma 16.2 from Adam Bocchner notes is equivalent to our statement above. You can use any of these versions of Gauss Lemma for Question 2 from Homework 2.

Exercise. Calculate $\frac{3}{5}$ usig the Gauss Lemma.

Solution. Our $p = 5$ and $a = 3$. Notice that $\frac{p-1}{2} = 2$, so our set $S = \{3, 3{\cdot}2\} = \{3, 6\}$. We now construct set $S' = \{3, 1\}$, since $6 \equiv 1 \mod 5$. Notice that S' has one element which is larger than $\frac{5}{2}$, so for us $n = 1$. Therefore $(\frac{3}{5}) = (-1)^1 = -1$. It follows that 3 is not a quadratic residue modulo 5.

Introduction to Number Theory.

Agata Smoktunowicz

12th March 2019

Lecture 15

Plan of Lecture 15

In this lecture we introduce finite fields by considering the following points.

- Definition of a field.
- $\mathbb{Z}$ is a field.
- Characteristic of a field.
- Prime subfields.

Definition of a field. A field is a commutative ring in which every nonzero element has a multiplicative inverse. In other words, if $a \neq 0$ then there is an element, denoted by a^{-1}, such that $a \cdot a^{-1} = a^1 \cdot a = 1$.

Proposition 1. Let p be a prime number. Then each nonzero element in $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is invertible, i.e. there exists an element $b \in \mathbb{Z}_p$ such that $ab \equiv 1 \mod p$.

Proof. By Fermat's Little theorem, $a^{p-1} \equiv 1 \mod p$, so we can take $b = a^{p-2}$.

Corollary. For each prime number p, $\mathbb{Z}_p$ is a field. We denote this field by F_p.

Exercise 1. Let F be a field and $a, b \in F$ be such that $a \neq 0, b \neq 0$. Show that $ab \neq 0$.

Solution. Suppose, on the contrary, that $a \neq 0, b \neq 0$ and $ab = 0$. Let a^{-1} be the inverse of a, then $a^{-1}(ab) = a^{-1} \cdot 0$. By the associativity of multiplication in a ring, we get $a^{-1}(ab) = (a^{-1}a)b = 1 \cdot b = b$. Also, it can be easily shown that in any ring $a^{-1} \cdot a = 0$, and it follows that $b = 0$, a contradiction.

Exercise 2. Let $n > 1$. Show that $\mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$ is not a field.

Solution. As usual, we will denote elements of $\mathbb{Z}_{p^n}$ as $\bar{0}$, $\bar{1}$, $\ldots p^n \bar{-} 1$. All these elements are pairwise distinct, so $\bar{p}^{n-1} \neq \bar{0}$. Observe that $\bar{p}^{n-1} \cdot \bar{p}^{n-1} = \bar{p}^{2n-2} = \bar{\neq} 0$.

Therefore, a product of two nonzero elements from $\mathbb{Z}_{p^n}$ is the zero element in $\mathbb{Z}_{p^n}$, so by Exercise 1 we obtain that $\mathbb{Z}_{p^n}$ is not a field.

Definition. A **subfield** of a field F is a subset $K \subseteq F$ containing 0 and 1 which is closed under the arithmetic operations addition, subtraction, multiplication and division (by non-zero elements).

Lemma 1. Let F be a finite field of characteristic p, then F_p is a subfield of F.

Proof. Every field contains the identity element $1 = 1_F$. Let $S = \{1, 1+1, 1+1+1, \ldots, 1+1+\ldots+1 = 0\}$, where the last element is the sum of p-copies of 1. Observe that S is closed under the operations of $+, -, \cdot$. Moreover, similarly as in Proposition 1 it can be shown that every element in S has a multiplicative inverse. So S is a field. Notice that the map $f : S \to Z_p$ given by $f(1_F) = 1_{\mathbb{Z}_p}$ is a homomorphism of rings, which is bijective, so S is isomorphic to $F_p = \mathbb{Z}_p$.

Proposition 2. Suppose that F is a field. Then F contains a smallest subfield P. This subfield P is contained in every subfield of F. We call this subfield P a prime subfield.

Proof. Notice that an intersection of any number of subfields is also a subfield. Moreover, since every subfield contains the identity element in F then the intersection also contains this identity element, so is nonzero. Observe that the intersection of subfields of F is a subfield P contained in every other subfield.

Theorem 1. Let F be a field of characteristic p. Then F has exactly p^n elements, for some natural number n.

Proof. By Lemma 1, F_p is a subfield of F. Notice that F is a vector space over the field F_p (so we can call elements of F vectors). We can find a basis $f_1, \ldots, f_n$ of this vector space F_p over F. It follows that each element a of F can be uniquely expressed in the form

$$a = k_1 f_1 + k_2 f_2 + \ldots + k_n f_n,$$

for some $k_1, k_2, \ldots, k_n \in F_p$. Observe that since F_p has p elements, then every element k_i can be chosen in p ways. So the total number of elements in F is p^n.

Introduction to Number Theory.

Agata Smoktunowicz

15th March 2019

Lecture 16

Plan of Lecture 16

- Learn about connections between generators in groups and primitive roots.
- Initially we will follow pages 35 and 36 from Adam Boocher's notes.
- All considered groups are abelian.

Definition. Let G be a group. We say that an element $g \in G$ generates G if the set of powers of g and g^1 is equal to all of G. If such a g exists, we say that G is cyclic and we write $G =< g >$.

Denition. If $g \in G$, we say that the order of g is the smallest positive integer n such that $g^n = 1$.

Corollary. Let G be a finite group which is cyclic. Then $g \in G$ is a generator of G if and only if the order of g equals $|G|$ the cardinality of G.

Lemma. Let G be a group and $g \in G$. If for integers m, n, we have $g^m = 1$ and $g^n = 1$, then $gcd(m, n) = 1$.

Proof. We know that $gcd(m, n)$ can be written as $mx + ny = gcd(m, n)$, we see that $g^{gcd(m,n)} = (g^m)^x(g^n)^y = 1$.

Theorem 1. Let G be a finite cyclic group of cardinality N. If $g \in G$ then the order of g divides N.

Proof. Let ξ be a generator of G, then the order of ξ equals $|G|$, so $\xi^{|G|} = 1$. Since g is a power of ξ we get $g^{|G|} = 1$. Let m denote the order of g. Suppose that m does not divide N. Then $gcd(m, N) < m$. But then by the previous proposition $gcd(m, N) = 1$. This however is contradictory, since by assumption we assumed that m was the smallest positive integer$k$ such that $g^m = 1$.

Remark. Theorem 1 is also true without the assumption that G is cyclic, and it is called the Lagrange theorem in group theory.

Theorem 2. Let G be a cyclic group and g be a generator of G. Let α be an integer, then element g^α is a generator of G if and only if $gcd(\alpha, |G|) = 1$, where $|G|$ denotes the cardinality of G.

Proof. Suppose that $gcd(\alpha, |G|) > 1$, and let $d = \frac{|G|}{gcd(\alpha,|G|)}$, then $(g^\alpha)^d = g^{|G|} = 1$. Since $d < |G|$ it follows that g^α is not a generator of G (as the order of a generator of G must be $|G|$).

Suppose now that $gcd(\alpha, |G|) = 1$, and let i be the order of g^α. Notice that $1 = (g^\alpha)^i = g^{\alpha \cdot i}$, and so $|G|$ divides $\alpha \cdot i$ (because the order of g is $|G|$, since G is a generator of G). Since α is coprime with $|G|$ it follows that $|G|$ divides i, so $|G| \leq i$, and so $|G| = i$ (by Theorem 1 $i \leq |G|$). Since the order of g^α is $|G|$ it follows that g^α is a generator of G.

Corollary 1. Let G be a finite group which is cyclic. Then G has $\phi(|G|)$ generators.

Remark. The group of units in $\mathbb{Z}_n$ is denoted as $\mathbb{Z}_n^*$.

Exercise 1. Let n be a natural number. How many elements has the group $\mathbb{Z}_n^*$?

Solution. Let $q \in \{0, 1, 2, \ldots, n-1\}$ and let $\bar{q}$ be the coset of q in Z_n. Observe that $\bar{q}$ is a unit in Z_n if and only if q is coprime with n. Therefore there are exactly $\phi(n)$ cosets which are units in $\mathbb{Z}_n$. Therefore the group of units $\mathbb{Z}_n^*$ has exactly $\phi(n)$ elements.

Theorem 3. Let n be a natural number such that the group $\mathbb{Z}_n^*$ is cyclic. Let ξ be an integer. Then ξ is a primitive root for n if and only if $\bar{\xi}$ is a generator of group $\mathbb{Z}_n^*$, where $\bar{\xi}$ denotes the coset of ξ in Z_n.

Proof. If ξ is a primitive root for n then $\xi^{\phi(n)} \equiv 1 \mod n$ and $\xi^i \mod n \neq 1 \mod n$ for $0 < i < \phi(n)$. So $\bar{\xi}$ has order $\phi(n)$ in the group $\mathbb{Z}_n^*$. By Exercise 1, $\phi(n)$ is the cardinality of $\mathbb{Z}_n^*$, so ξ is a generator of $\mathbb{Z}_n^*$.

If $\bar{\xi}$ is a generator of $\mathbb{Z}_n^*$, then $\bar{\xi}$ has order equal to $|\mathbb{Z}_n^*| = \phi(n)$. Therefore $\bar{\xi}^{\phi(n)} = \bar{1}$ and $\bar{\xi}^i \neq \bar{1}$ for $0 < i < \phi(n)$. Therefore $\xi^{\phi(n)} \equiv 1 \mod n$ and $\xi^i \mod n \neq 1 \mod n$ for $0 < i < \phi(n)$. So $\bar{\xi}$ is a primitive root for n.

Exercise. Suppose that $\mathbb{Z}_n$ has a primitive root. How many primitive roots are in $\mathbb{Z}_n$ which are in the interval $[0, n]$?

Solution. By Theorem 3 it is equivalent to ask: How many generators has the group $\mathbb{Z}_n^*$? By Exercise 1, the cardinality of the group $\mathbb{Z}_n^*$ is $\phi(n)$. By Corollary 1 the group $\mathbb{Z}_n^*$ has $\phi(\phi(n))$ generators, so the answer is $\phi(\phi(n))$.

Introduction to Number Theory.

Agata Smoktunowicz

19th March 2019

Lecture 17

During Lecture 17 we proved Theorem 4.5.1 from the book ”Rings, Fields and Groups” by R.B.J.T. Allenby, 2001.

Theorem 4.5.1

Let p be a positive prime and n a positive integer. Then there exists a field with exactly p^n elements.

Lecture 17 is not required for the exam so it is not provided in detail.

Introduction to Number Theory.

Agata Smoktunowicz

22nd March 2019

Lecture 18

Plan of Lecture 18

- Hensel's Lemma.
- Exercises related to Hensel's Lemma.

Hensel's Lemma

Let $f(x)$ be a polynomial with integer coefficients. Let p be a prime number. Let k be a positive integer, and r be an integer such that

$$f(r) \equiv 0 \mod p^k.$$

If $f'(r)$ is not divisible by p then there is an integer s such that

$$f(s) \equiv 0 \mod p^{k+1}$$

and

$$s \equiv r \mod p^k.$$

Moreover, s is unique modulo p^{k+1}.

Proof. We gave an intuitive proof of Hensel's Lemma - we didn't give a formal proof. The formal proof can be found on page 30 of Adam Boocher's notes, it is the proof of Theorem 7.3 (a) on page 26.

We did the following exercise from "Number theory in exercises", PWN by Jerzy Rutkowski:

Exercise. How many solutions has the congruence

$$x^3 + x^2 + 29 \equiv 0 \mod 25.$$

Solution. We first calculate the number of solutions modulo 5:

$$x^3 + x^2 + 29 \equiv 0 \mod 5.$$

By checking all possibilities modulo 5 we see that the only solution is $3 \mod 5$. We will apply Hensel's Lemma for $p = 5$, $k = 1$, $f(x) = x^3+x^2+29$. Notice that $f'(x) = 3x^2+2x$. Observe that $f'(3) = 27+6 = 33$ is not divisible by $p = 5$. Therefore we can apply Hensel's Lemma: it follows that solution $x = 3 \mod 5$ can be uniquely lifted to a solution modulo 25, therefore there is exactly one solution modulo 25 of the equation $x^3 + x^2 + 29 \equiv 0 \mod 25$.

Introduction to Number Theory.

Agata Smoktunowicz

26th March 2019

Lecture 19

Plan of Lecture 19

- A modification to Hensel's lemma for application when $f'(r)$ is divisible by p.
- Exam topics.

A modified version of Hensel's Lemma

Let $f(x)$ be a polynomial with integer coefficients. Let p be a prime number. Let k be a positive integer and r be an integer such that

$$f(r) \equiv 0 \mod p^k.$$

If $f'(r)$ is divisible by p then

$$f(s) \equiv f(r) \mod p^{k+1}$$

for every s such that $s \equiv r \mod p^k$. In particiular, the following holds:

1. If $f(r) \equiv 0 \mod p^{k+1}$, then there are exactly p solutions s modulo p^{k+1} such that

   $$f(s) \equiv 0 \mod p^{k+1}$$

   and

   $$s \equiv r \mod p^k.$$

2. If $f(r)$ is not divisible by p^{k+1} then there are no solutions s such that

   $$f(s) \equiv 0 \mod p^{k+1}$$

   and

   $$s \equiv r \mod p^k.$$

Proof. It follows because for $s = r + tp^k$ we have $f(s) = f(r) + tp^k f'(r) + p^{k+1}e$ for some $e \in \mathbb{Z}$ by Taylor's expansion formula. We didn't give a formal proof of this modification of Hensel's lemma. For students interested in understanding the proof the formal proof can be found on page 30 of Adam Boocher's notes, it is the proof of Theorem 7.3 on page 26.

We did the following exercise from "Number theory in exercises", PWN by Jerzy Rutkowski:

Exercise 1. Find how many solutions modulo 7^2 has congruence

$$x^2 + 4x + 18 \equiv 0 \mod 49.$$

Solution. We first find solutions modulo 7. Denote $f(x) = x^2+4x+18$. We calculate that $f(0), f(1), f(2), f(3), f(4), f(6)$ are not divisible by 7 and

$$f(5) \equiv 0 \mod 7.$$

We calculate $f'(x) = 2x+4$, $f'(5) = 14$ is divisible by 7. So there is only one solution modulo 7, and it is 5 modulo 7. By the above modification of Hensel's lemma there are either 7 solutions modulo 49 or there are no solutions s such that $f(s) \equiv 0 \mod 49$ (since then $f(s) = 0 \mod 7$ so $s = 5 \mod 7$). Observe that $f(5) = 25 + 20 + 18 = 63$ is not divisible by 49, so there are no solutions x to congruence $x^2 + 4x + 18 \equiv 0 \mod 49$.

We also did the following exercise:

Exercise 2. Find how many solutions modulo 25 has congruence

$$x^4 \equiv 0 \mod 25.$$

Solution. We first find solutions modulo 5. Denote $f(x) = x^4$. We calculate $f(0) \equiv 0 \mod 5$ and $f(1), f(2), f(3), f(4)$ are not divisible by 5. So there is only one solution modulo 5, and it is 0 modulo 5. Now the above modificaton of Hensel's lemma yields that there are either 5 solutions modulo 25 to the congruence $x^4 \equiv 0 \mod 25$ or there are no solutions. Since $x = 0$ is a solution the latter possibility is not possible, so we have exactly 5 solutions modulo 25.

We also discussed the exam topics. The exam topics are as follows:

Exam topics

1. Euclidean algorithm and its applications.

2. Chinese Remainder Theorem.

3. The Euler function $\phi(n)$.

4. Fermat's Little theorem, Euler's theorem, Wilson's theorem.

5. Gaussian integers $\mathbb{Z}[i]$.

6. Legendre symbol, quadratic residues.

7. Primitive roots in $\mathbb{Z}_p$, where p is a prime number.

8. Hensel's lemma.

9. Finding how many solutions modulo n there are to a congruence $f(x) \equiv 0 \mod n$ where n is an integer and $f(x)$ is a polynomial with integer coefficients.

Comments about the exam.

1. You may be asked to give the definitions of some notions (for example of a Gaussian integer).

2. You may be asked to give statements of some theorems and lemmas or results that we proved during our lectures, for example to state Fermat's Little theorem (but I will not ask you to prove them - notice though that knowing the general idea of a proof can be useful).

3. 50% of the exam questions are standard and very similar to exercises which we did during the lectures, homeworks and tutorials (for example but with different numbers).

4. There will be five questions, each divided into a small number of parts. The total number of exam marks is 50, but please note that THE MARKS ARE NOT EQUALLY DISTRIBUTED ACROSS THE FIVE QUESTIONS.

5. There will be a question for every exam topic listed above.

6. Please answer all questions.

7. Only the material covered during the lectures, tutorials and homeworks are compulsory for the exam.

Introduction to Number Theory.

Agata Smoktunowicz

29th March 2019

Lecture 20

This lecture has been provisionally rescheduled for the 11th May. It will probably be a revision lecture and/or an opportunity for students to raise any difficulties they may be having with the course content. The details will be decided in lecture 21 on Tuesday, April 2nd.

Introduction to Number Theory
Lecture 21

MOCK EXAM

2nd April 2019

Introduction to Number Theory - Mock Exam

2nd April, 2019

You can use any result from the tutorials and the lectures if you properly state it.

Question 1

1. [**4 marks**] Find all solutions $x \in \mathbb{Z}$ to the congruence

$$377x = 1 \mod 416.$$

2. [**4 marks**] Solve the system of congruences

$$x \equiv 3 \mod 100$$

$$x \equiv 53 \mod 75$$

in integers $x \in \mathbb{Z}$.

Question 2

1. [**3 Marks**] State Wilson's theorem.
2. [**3 mark**] Use Wilson's theorem to calculate the last decimal number of $4! + 1$.
3. [**4 marks**] Let $\phi(n)$ be Euler's function. Let $n > 1$ be an odd natural number. Show that $\phi(2n) = \phi(n)$.
4. [**2 marks**] Give an example of a natural number $n > 1$ such that $\phi(2n) \neq \phi(n)$.

Question 3
Recall that $i = \sqrt{-1}$.

1. [**2 Marks**] Give the definition of a prime Gaussian integer.
2. [**4 Marks**] Determine whether $1 + 2i$ is an irreducible Gaussian integer.
3. [**4 Marks**] Determine whether 67 is a prime Gaussian integer.

Question 4

1. **[3 marks]** Let $p, q > 0$ be odd prime numbers. Let $(\frac{q}{p})$ denote the Legendre symbol. State the quadratic reciprocity theorem.

2. **[3 marks]** Calculate $(\frac{7}{41})$.

3. **[2 marks]** Let $a \in Z$, $a > 0$. Show that $(\frac{a^2}{p}) = (\frac{a^4}{p})$ for every prime number $p > 0$.

4. **[6 marks]** Let p be a prime number and let $\xi \in \mathbb{Z}$ be such that ξ^ξ is a primitive root for $\mathbb{Z}_p$ and $\xi > 1$. Show that ξ is a primitive root in $\mathbb{Z}_p$.

Question 5

1. **[6 marks]** How many solutions modulo 81 has the congruence

$$x^4 + 2x^2 + 2x \equiv 5 \mod 81.$$

You do not need to find the solutions.

Solutions

- Find all solutions $x \in \mathbb{Z}$ to the congruence

$$377x = 13 \mod 416.$$

It suffices to find integers x, y such that $317 \cdot x + 416 \cdot y = d$ (we actually only need x, so we are doing more than is required here).

By the Euclidean Algorithm,

$$416 = 377 + 39$$

$$377 = 39 \cdot 9 + 26$$

$$39 = 26 + 13$$

$$26 = 13 \cdot 2 + 0.$$

The last non-zero reminder is 13, therefore $(416, 377) = 13$.

Now, working back, we get

$$416 - 377 = 39$$

$$377 - 39 \cdot 9 = 26$$

$$39 - 26 = 13.$$

We get $13 = 39 - 26 = (416 - 377) - (377 - 39 \cdot 9) = 416 - 2 \cdot 377 + 9 \cdot 39 = 416 - 2 \cdot 377 + 9 \cdot (416 - 377) = 10 \cdot 416 - 11 \cdot 377$. Thus $x = -11, y = 10$ is a solution. We know that the solution will be of the form $x = -11 + \frac{377}{13}t = -11 + 29t$ and $y = 10 - \frac{416}{13}t = 10 - 32t$ for $t \in \mathbb{Z}$. Therefore the solution to our congruence is $x = -11 + 29t$ for $t \in \mathbb{Z}$.

- Solve the system of congruences

$$x \equiv 3 \mod 100$$

$$x \equiv 53 \mod 75.$$

in integers $x \in \mathbb{Z}$.

We first recall a remark from Lecture 9: "Knowing a number $x \mod N$ is equivalent to knowing $x \mod$ each of the prime powers $p_j^{e_j}$ in $N = p_1^{e_1} \cdots p_n^{e_n}$. For example knowing that $x \equiv 27 \mod 30$ is the same as knowing $x \equiv 1 \mod 2$, $x \equiv 0 \mod 3$, $x \equiv 2 \mod 5$."

By this remark it suffices to solve:

$$x \equiv 3(\mod 4), x \equiv 3(\mod 25)$$
$$x \equiv 53(\mod 25), x \equiv 53(\mod 3).$$

Notice that if $x \equiv 3(\mod 25)$ then $x \equiv 53(\mod 25)$, so we only need to solve the three congruences:

$$x \equiv 3(\mod 4),$$
$$x \equiv 53(\mod 25),$$
$$x \equiv 53(\mod 3).$$

It is equivalent to solve the following congruences:

$$x \equiv 3(\mod 4),$$
$$x \equiv 3(\mod 25),$$
$$x \equiv 2(\mod 3).$$

You can use the fact that $12 \cdot (-2) \equiv 1 \mod 25$.

We can now apply the Chinese remainder theorem method for $m_1 = 4, m_2 = 25, m_3 = 3$, $a_1 = 3$, $a_2 = 3$, $a_3 = 2$.

We find $N = m_1 \cdot m_2 \cdot m_3 = 300$, $N_1 = \frac{N}{m_1} = 75$, $N_2 = \frac{N}{m_2} = 12$, $N_3 = \frac{N}{m_3} = 100$. We find solutions to congruences $N_i x_i \equiv 1 \mod m_i$: $75x_1 \equiv 1 \mod 4$ (which is equivalent to $-x_1 \equiv 1 \mod 4$), $12x_2 \equiv 1 \mod 25$, $100x_3 \equiv 1 \mod 3$ (which is equivalent to $x_3 \equiv 1 \mod 3$). We can take $x_1 = -1$, $x_2 = -2$, $x_3 = 1$.

A solution is $x \equiv a_1x_1N_1 + a_2x_2N_2 + a_3x_3N_3 = 3 \cdot (-1) \cdot 75 + 3 \cdot (-2) \cdot 12 + 2 \cdot 1 \cdot 100(\mod 300) \equiv -225 - 72 + 200(\mod 300) \equiv -97(\mod 300)$.

Question 2

- State Wilson's theorem.

Let $p > 0$ be a prime number, then $(p-1)! + 1$ is divisible by p.

- Calculate the last decimal number of $4! + 1$.

  By Wilson's theorem $4!+1$ is divisible by 5. It is an odd number, so the last decimal number is 5. Or it can be calculated by hand, $4! + 1 = 25$.

- Let $\phi(n)$ be the Euler's function. Let $n > 1$ be an odd natural number. Show that $\phi(2n) = \phi(n)$.

  By a formula from the lectures we get that iff $p_1, p_2, \ldots, p_j$ are distinct primes that divide n and $n = p_1^{\alpha_1} \cdots p_j^{\alpha_j}$ then

  $$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}).$$

  Since n is odd $2, p_1, p_2, \ldots, p_j$ are distinct primes that divide n and $n = 2p_1^{\alpha_1} \cdots p_j^{\alpha_j}$. Consequently:

  $$\phi(2n) = (2-1)(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) = \phi(n).$$

- Give an example of a natural number $n > 1$ such that $\phi(2n) \neq \phi(n)$.

  $n = 2$. By the above formula, $\phi(2) = 1$ and $\phi(2 \cdot n) = \phi(4) = 2$.

Question 3
Recall that $i = \sqrt{-1}$.

- Give the definition of a prime Gaussian integer.

  If a is neither zero nor a unit in $\mathbb{Z}[i]$ we say that a is prime in $\mathbb{Z}[i]$ if whenever $a|cd$ with $c, d \in \mathbb{Z}$ it follows that $a|c$ or $a|d$. (If $u|1$ then u is a unit in $\mathbb{Z}$.)

- Determine whether $1 + 2i$ is an irreducible Gaussian integer.

  Observe that if $1 + 2i = (a + bi)(c + di)$, then we can take absolute values of these complex numbers and get $\sqrt{1 + 2^2} = \sqrt{a^2 + b^2}\sqrt{c^2 + d^2}$. We can take the square of both sides of this equation to get $5 = (a^2 + b^2)(c^2 + d^2)$. It follows that either $a^2 + b^2 = 1$ or $c^2 + d^2 = 1$, hence either $a + bi$ is a unit or $c + di$ is a unit in $\mathbb{Z}[i]$. It follows that $1 + 2i$ is an irreducible Gaussian integer.

- Determine whether 67 is a prime Gaussian integer.

  Notice that $67 = 3 + 4 \cdot 16$. Moreover, 67 is a prime integer. By Theorem 4 from Lecture 4 a Gaussian integer is a prime Gaussian integer if and only if it is an irreducible Gaussian integer. We will show that 67 is a prime Gaussian integer. It suffices to show that 67 is an irreducible Gaussian integer. Suppose on the contrary, that 67 can be written as $67 = (a + bi)(c + di)$ where $a, b, c, d \in \mathbb{Z}$ and $a + bi, c + di$ are not units in the ring of Gaussian integers. Notice that by Lemma 1 from Lecture 4 the norm of a non-unit is larger than one, so $|a + bi| > 1, |c + di| > 1$. Notice that $67 = (a + bi)(c + di)$ implies $67^2 = |a + bi|^2|c + di|^2 = (a^2 + b^2)(c^2 + d^2)$. It follows that $a^2 + b^2 = 67$ and $c^2 + d^2 = 67$. Notice that $a^2, b^2 \in \{4k + 1, 4k : k \in \mathbb{Z}\}$, therefore $a^2 + b^2 \in \{4t, 4t + 1, 4t + 2 : t \in \mathbb{Z}\}$. It follows that $a^2 + b^2 \neq 67$. We have obtained a contradiction. It follows that 67 is an irreducible Gaussian integer, and hence a prime Gaussian integer.

Question 4

- Let $p, q > 0$ be odd prime numbers. Let $(\frac{q}{p})$ denote the Legendre symbol. State the quadratic reciprocity theorem.

  Quadratic reciprocity, part 1: Let $p, q > 0$ be distinct odd primes, then

  $$(\frac{p}{q}) = (\frac{q}{p})$$

  provided that either $p \equiv 1(\mod 4)$ or $q \equiv 1(\mod 4)$.

  Quadratic reciprocity, part 2: Let $p, q > 0$ be distinct odd primes, then

  $$(\frac{p}{q}) = -(\frac{q}{p})$$

  provided that $p \equiv 3(\mod 4)$ and $q \equiv 3(\mod 4)$.

  Recall that The Legendre symbol of a modulo p is $(\frac{a}{p})$. It is 1 if $a \equiv r^2(\mod p)$ for some integer r and -1 otherwise. If $(\frac{a}{p}) = 1$ then we say that a is a quadratic residue modulo p.

- Calculate $(\frac{7}{41})$.

  We will use a theorem from Lecture 10 related to the Legendre symbol. By the quadratic reciprocity law $(\frac{7}{41}) = (\frac{41}{7})$. Notice that $(\frac{41}{7}) = (\frac{7 \cdot 6 - 1}{7}) = (\frac{-1}{7})$. We know that $(\frac{-1}{7}) = (-1)^{\frac{7-1}{2}} = -1$. Therefore $(\frac{7}{41}) = -1$.

- Let $a \in Z$, $a > 0$. Show that $(\frac{a^2}{p}) = (\frac{a^4}{p})$ for every prime number $p > 0$.

  By the definition of the Legendre symbol we have two possibilities, either $(\frac{a}{p}) = 1$ or $(\frac{a}{p}) = -1$. In both cases we have $(\frac{a^2}{p}) = (\frac{a}{p})^2 = 1$ and $(\frac{a^4}{p}) = (\frac{a}{p})^4 = 1$.

- Let p be a prime number and let $\xi \in \mathbb{Z}$ be such that ξ^ξ is a primitive root for $\mathbb{Z}_p$ and $\xi > 1$. Show that ξ is a primitive root in $\mathbb{Z}_p$.

  Since ξ^ξ is a primitive root for $\mathbb{Z}_p$, it follows that for every $i \in \mathbb{Z}$ which is not divisible by p there is a natural number α such that $i \equiv (\xi^\xi)^\alpha \mod p$.

  Therefore for every $i \in \mathbb{Z}$ which is not divisible by p there is a natural number β such that $i \equiv \xi^\beta \mod p$ (for example $\beta = \alpha \cdot \xi$. This implies that ξ is a primitive root for $\mathbb{Z}_p$, since then ξ is a generator for $\mathbb{Z}_p$.

Question 5

- How many solutions modulo 81 has the congruence:

  $$x^4 + 2x^2 + 2x \equiv 5 \mod 81.$$

  You do not need to find the solutions.

  Notice that $81 = 3^4$. We first find solutions modulo 3, that is, solutions of the congruence $f(x) \equiv 0 \mod 3$ where $f(x) = x^4 + 2x^2 + 2x - 5$. To find solutions we calculate $f(0) = -5$, $f(1) = 0$, $f(2) = -4$, so the only solution modulo 3 is $x \equiv 0 \mod 3$.

We calculate $f'(x) = 4x^3 + 2x + 2$. Notice that $f'(1) = 8$ is not divisible by 3, therefore we can apply Hensel's Lemma to find that there is exactly one solution s modulo 9 such that $s \equiv 1 \mod 3$. Notice that $f'(s)$ is not divisible by 3 because $s = 1+3t$ for some integer t and $f'(1)$ is not divisible by 3. Therefore we can extend solution s to the unique solution s' modulo 27 such that $f(s') \equiv 0 \mod 27$ and $s' \equiv s \mod 9$. Hence s' is divisible by 3 and $f(s')$ is not divisible by 3 (because $f'(s)$ is not divisible by 3 and $s' - s$ is divisible by 3). By applying Hensel's lemma one more time, we get that there is exactly one integer s'' modulo 81 such that $f(s'') \equiv 0 \mod 81$.

Introduction to Number Theory.

Agata Smoktunowicz

5th April 2019

Lecture 22

Plan of Lecture 22

- A modification to Hensel's lemma when we need to apply Hensel's lemma several times.
- An exercise on Gaussian integers.

A modified version of Hensel's Lemma

Let $f(x)$ be a polynomial with integer coefficients. Let p be a prime number. Let k be a positive integer and r be an integer such that

$$f(r) \equiv 0 \mod p^k.$$

Let $N > 0$ be an integer. If $f'(r)$ is not divisible by p then there is an integer s_N such that

$$f(s_N) \equiv 0 \mod p^{k+N}$$

and

$$s_N \equiv r \mod p^k.$$

Moreover, s_N is unique modulo p^{k+N}.

Proof. After applying Hensel's lemma N times we get the required result. We only need to show that we can apply Hensel's lemma again as the derivative $f'(s_i)$ is not divisible by p (so the assumptions of Hensel's lemma hold): Notice that since $s \equiv r \mod p$ it follows that $f'(s)$ is divisible by p if and only if $f'(r)$ is divisible by p. So we can apply Hensel's lemma again. We can continue applying Hensel's lemma as at i-th step we have that $f'(s_i)$ is divisible by p if and only if $f'(r)$ is divisible by p. It is because $s_i - r$ is divisible by p, so we can write $s_i = r + tp$ and notice that that by Taylor's expansion formula applied to the polynomial $f'(x)$ we have $f'(s_i) = f'(r) + tpf''(r) + p^2e$ for some $e \in \mathbb{Z}$.

Exercise. How many solutions modulo 2^6 has the congruence

$$x^2 + x + 4 \equiv 0 \mod 2^6?$$

Proof. We will apply the modified Hensel's lemma from above. For us $p = 2, k = 1$, $f(x) = x^2 + x + 4$. We calculate the number of solutions modulo 2 to the congruence $f(x) \equiv 0 \mod 2$, the solutions are $x_0 = 1$ and $x_0 = 0$. To apply Hensel's lemma we calculate $f'(x) = 2x + 1$ at points $x = 0$ and $x = 1$, $f'(0) = 1$ and $f'(1) = 3$, they are not divisible by $p = 2$ so we can apply Hensel's lemma.

So for each x_0 ($x_0 = 1$ or $x_0 = 0$) there is a unique extension to a unique solution modulo 2^6. So there are exactly 2 solutions modulo 2^6.

Exercise 2 Solve the congruence:

$$x^3 + x^2 + 29 \equiv 0 \mod 25.$$

Solution. We first calculate number of solutions modulo 5, to the congruence

$$x^3 + x^2 + 29 \equiv 0 \mod 5.$$

We find that $x \equiv 3 \mod 5$ is a solution, and that there are no more solutions modulo 5.

We calculate $f'(3) = 3 \cdot 3^2 + 2 \cdot 3 = 33$, it is not divisible by 5, so we can apply Hensel's lemma.

By Hensel's lemma there is exactly one solution modulo 25 to the congruence $x^3 + x^2 + 29 \equiv 0 \mod 25$, and it is a lift of the solution $x = 3 \mod 5$. So this solution is of the form $y \equiv 3 + 5t \mod 25$.

We will use the following fact:

$$f(x_0 + tp) = f(x_0) + tpf'(x) + p^2 e$$

for some $e \in \mathbb{Z}$ (this follows from the Taylor extension formula), where our $p = 5$. So if $y = 3 + 5t$ then

$$f(y) = f(3 + 5t) = f(3) + 5tf'(x) + 25e$$

for some $e \in \mathbb{Z}$. Notice that $f(y) \equiv 0 \mod 25$ implies $f(3) + 5tf'(3) \equiv 0 \mod 25$. It follows that $f(3) + tf'(3) \equiv 0 \mod 25$ so $65 + 5t \cdot 33 \equiv 0 \mod 25$, hence $13 + t \cdot 33 \equiv 0 \mod 5$, so $t \equiv -1 \mod 5$. It follows that $y \equiv 3 + 5t \mod 25 \equiv 3 - 5 \mod 25 = -2 \mod 25$. Hence $y = -2 \mod 25$ is the unique solution modulo 25 to the congruence $x^3 + x^2 + 29 \equiv 0 \mod 25$.

Gaussian integers

Exercise. Let a, z be Gausian integers, $a \neq 0$. Show that if a is a divisor of z in $\mathbb{Z}[i]$ then $|a|^2$ divides $|z|^2$ in $\mathbb{Z}$, where $|x + iy| = \sqrt{x^2 + y^2}$ for $x, y \in \mathbb{Z}$.

Proof. Notice that a divides z as a Gaussian integer means that $a \cdot p = z$ for some $p \in \mathbb{Z}[i]$. We can take the absolute value on both sides to get $|a| \cdot |p| = |ap| = |z|$. By taking squares of both sides we get $|a|^2 \cdot |p|^2 = |ap| = |z|^2$, all elements $[a|^2, |p|^2, |z|^2$ are integers, so $|a|^2$ divides $|z|^2$ as an integer.