7th Lecture: 3/2

The second part of the course serves as an introduction to both *number theory* and to *abstract algebra* (groups, rings, modules, fields). The focus is primarily on the latter, since a grounding in abstract algebra is useful for more advanced studies in mathematics more generally. We will, however, show how some classical material in number theory can be presented using this abstract algebraic language and machinery.

A large part of the corpus of knowledge in number theory deals with *prime numbers*. In our first lecture, we will present the two most fundamental results about these: the *infinitude of primes* and the *uniqueness of prime factorisation* (the so-called *Fundamental Theorem of Arithmetic (FTA)*). These were already proven in Euclid's Elements and those proofs remain state-of-the art. Hence, this first lecture does not use any of the abstract algebraic machinery developed subsequently and so this set of notes can be read independently of what follows. Note, however, three things:

(i) *Euclid's algorithm*, which is the key tool for proving FTA, will also be employed later on, for computing inverses in finite modular groups $\mathbb{Z}_n^\times$ (see Lecture 9).

(ii) The notion of "prime factorisation" can be generalised from the integers to so-called *algebraic number rings*. The study of these comprises the subject known as *Algebraic Number Theory*. Familiarity with the general techniques of abstract algebra is needed if one wants to pursue study in that direction. In particular, the FTA can be generalised to those algebraic number rings which are so-called *unique factorisation domains*, a subset of which belong to the class of *Euclidean rings*.

(iii) For further study in abstract algebra one is recommended to take the course *Algebraic Structures* offered by the math department. For further studies in number theory, there are Master's level courses in *Algebraic Number Theory* and *Analytic Number Theory*. In more recent times, the subject of *Combinatorial Number Theory* has also become a recognised field in its own right.

Prime Numbers. I will assume familiarity with some basic concepts, definitions, notation, terminology and results from elementary number theory. Consult Chapter 3 of Vol. 1 of the course book if necessary.

Definition 7.1. A positive integer $p \in \mathbb{Z}_+$ is called a *prime number* if
(i) $p \geq 2$, and
(ii) the only positive divisors of p are 1 and p itself, in other words

$$a \in \mathbb{Z}_+ \ \wedge \ a \,|\, p \ \Rightarrow \ a = 1 \ \vee \ a = p.$$

Proposition 7.2. *Every positive integer can be written as a product of primes.*

PROOF: Strong induction on $n \in \mathbb{Z}_+$. $n = 1$ is an empty product of primes. Suppose each integer $1, 2, \ldots, n$ can be written as a product of primes and consider $n+1$.

Case 1: $n+1$ is prime. Then just write $n+1 = n+1$.

Case 2: $n+1$ is not prime. Then, by definition, there exist integers u, v such that $n+1 = uv$ and each of u and v is at most n. By the induction assumption, each of u and v is a product of primes. Concatenating these products gives a representation of

$n+1$ as a product of primes.

Theorem 7.3. (Infinitude of primes) *There are infinitely many primes.*

PROOF: Suppose the contrary. Then one can make a finite list of all the primes, say $p_1, p_2, \ldots, p_n$. Consider the number

$$N = \prod_{i=1}^{n} p_i \, + \, 1.$$

By construction, N leaves remainder one upon division by any p_i. Since each $p_i \geq 2$, this means N is not divisible by any p_i. But N has *some* prime factorisation, by Proposition 7.2. Hence, N must be divisible by some prime not on the list, which contradicts the assumed completeness of the list.

Theorem 7.4. (Fundamental Theorem of Arithmetic) *Every positive integer has a unique representation as a product of primes.*

By Proposition 7.2, it remains to prove uniqueness. The key lemma in the proof of FTA is the following:

Key Lemma 7.5. *Let p be a prime and let a, b by any positive integers. Then*

$$p \,|\, ab \;\Rightarrow\; p \,|\, a \;\vee p \,|\, b.$$

We postpone the proof of this result and first show how it leads to FTA. First we note a corollary:

Corollary 7.6. *Let p be a prime, let $n \geq 2$ and let $a_1, a_2, \ldots, a_n$ be any positive integers. Then*

$$p \,|\, \prod_{i=1}^{n} a_i \;\Rightarrow\; \bigvee_{i=1}^{n} p \,|\, a_i.$$

PROOF OF COROLLARY: Induction on n. The case $n = 2$ is Lemma 7.5. Suppose the corollary holds for some $n \geq 2$ and let $a_1, a_2, \ldots, a_{n+1}$ be positive integers such that p divides their product. Set $b_1 := \prod_{i=1}^{n} a_i$ and $b_2 := a_{n+1}$. Thus $p \,|\, b_1 b_2$ and so, by Lemma 7.5, either $p \,|\, b_1$ or $p \,|\, b_2$. In the latter case, $p \,|\, a_{n+1}$ and we are done. In the former case, we're saying that $p \,|\, \prod_{i=1}^{n} a_i$. But then by the induction assumption we have that $p \,|\, a_i$, for some $1 \leq i \leq n$, and again we are done.

PROOF OF THEOREM 7.4 ASSUMING COROLLARY 7.6: Let $n \in \mathbb{Z}_+$ and suppose we are given two representations of n as a product of primes, say

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{j=1}^{l} q_j^{\beta_j}. \tag{7.1}$$

Consider some p_i. In particular, (7.1) says that p_i divides the product of primes (which will include repititions whenever some $\beta_j > 1$, but that doesn't matter) $\prod_{j=1}^{l} q_j^{\beta_j}$.

Hence, by Corollary 7.6, there must be some q_j such that $p_i \,|\, q_j$. But both p_i and q_j are primes, so this means that $p_i = q_j$.

In other words, every prime in the first product in (7.1) must also appear in the second product and vice versa. It is then also easy to see (by induction, if you like) that the powers must also match, i.e.: $\alpha_i = \beta_i$ for each i. Hence, the two representations of n involve exactly the same prime powers, v.s.v.

So to complete the proof of Theorem 7.4, it remains to prove Lemma 7.5. It will in turn follow from the next result, Proposition 7.8 - note that the result is implicit in Euclid's Elements and that its modern name was only applied later (Bezout lived in the 18th century). First a definition, in case you've forgotten:

Definition 7.7. Let $a,\, b \in \mathbb{Z}_+$. The number $d \in \mathbb{Z}_+$ is called the *greatest common divisor* of a and b, and denoted GCD$(a,\, b)$, if

(i) d is a common divisor of a and b, i.e.: $d \,|\, a$ and $d \,|\, b$

(ii) it is the largest integer with this property, i.e.: if $c \,|\, a$ and $c \,|\, b$ then $c \leq d$.

Proposition 7.8. (Bezout's Lemma) *Let $a,\, b \in \mathbb{Z}_+$ and let d be their GCD. Then there exist $x,\, y \in \mathbb{Z}$ such that $ax + by = d$.*

PROOF OF LEMMA 7.5 ASSUMING PROPOSITION 7.8: We prove the logically equivalent, contrapositive statement, namely that if p divides neither a nor b then it doesn't divide ab either.

Since p doesn't divide a and p is prime, it must be the case that GCD$(p,\, a) = 1$. Hence, by Proposition 7.8, there exist integers $x,\, y$ such that

$$ax + py = 1. \tag{7.2}$$

Similarly, if p doesn't divide b then there must exist integers $z,\, w$ such that

$$bz + pw = 1. \tag{7.3}$$

Multiplying (7.2) and (7.3) together, we get

$$1 = (ab)(xz) + p(axy + bzw) + p^2(yw). \tag{7.4}$$

Now if p divided ab, then it would divide the whole RHS of (7.4). But then it would have to divide the LHS, namely 1, which it can't since $p \geq 2$. Hence, p doesn't divide ab, v.s.v.

So now we've reduced the complete proof of Theorem 7.4 to that of Proposition 7.8. The latter is due to the fact that Euclid's Algorithm finds the GCD of two given inputs a and b and, when run backwards, yields an explicit solution of $ax + by = d$. I will not write out the full proof of this for arbitrary a and b because it would be a lot of ordbajs. Instead, I will just show how things work for an example. Hence, after presenting and discussing that example, I consider the proof of Theorem 7.4 to be complete.

Example 7.9. (Euclid's algorithm) Let $a = 1368$, $b = 750$. We apply Euclid's algorithm to first find $d =$ GCD$(a,\, b)$ and then to find integers $x,\, y$ such that $ax + by = d$.

Step 1: Find d.

The algorithm is just repeated division-and-remainder computation.

$$\begin{aligned} 1368 &= 1 \cdot 750 + 618, \\ 750 &= 1 \cdot 618 + 132, \\ 618 &= 4 \cdot 132 + 90, \\ 132 &= 1 \cdot 90 + 42, \\ 90 &= 2 \cdot 42 + 6, \\ 42 &= 7 \cdot 6 + 0. \end{aligned}$$

The algorithm terminates once a remainder of zero is obtained. It is clear that this must happen after finitely may steps, since the remainders are strictly decreasing and non-negative. The claim is that the last non-zero remainder equals the GCD of the two original numbers. This is proven in two steps:

CLAIM 1: The last non-zero remainder is a common divisor of the two original numbers, a and b. To understand why, follow the above example *backwards* step-by-step. In the last step we get remainder zero, which means that the last non-zero remainder, 6 in this case, divides the previous remainder, 42 in this case. Now go to the second last step. That 6 divides 42 implies it divides the whole of the RHS. Hence it divides the LHS, 90 in this case, or the previous remainder in general. Now go to the previous step. Since 6 divides both 42 and 90, it must also divide 132. And so on. The last non-zero remainder is a divisor of every previous remainder. When we get to the top two steps, we deduce from the same reasoning that it divides the two original numbers, v.s.v.

CLAIM 2: Any common divisor of a and b must also divide the last non-zero remainder in Euclid's algorithm (see Remark 7.10 below). To see this, work your way *forwards* through the steps of the algorithm. Let c be a common divisor of a and b. The first step implies c will also divide the first remainder, in this example 618. Thus c divides both 750 and 618. From the second step, it now follows that 6 divides the next remainder 132. And so on. Any common divisor of a and b muast also divide each remainder computed by the algorithm. In particular, it divides the last non-zero remainder, v.s.v.

Step 2: Go backwards through the steps of the algorithm to obtain an expression $d = ax + by$.

In our example, the sequence of computations will look as follows:

$$\begin{aligned} 6 &= 90 - 2 \cdot 42 \\ &= 90 - 2(132 - 90) \\ &= 3 \cdot 90 - 2 \cdot 132 \\ &= 3(618 - 4 \cdot 132) - 2 \cdot 132 \\ &= 3 \cdot 618 - 14 \cdot 132 \\ &= 3 \cdot 618 - 14(750 - 618) \\ &= 17 \cdot 618 - 14 \cdot 750 \\ &= 17(1368 - 750) - 14 \cdot 750 \\ &= 17 \cdot 1368 - 31 \cdot 750. \end{aligned}$$

Hence we have written $d = ax + by$, with $x = 17$ and $y = -31$. It's clear that things will work out the same way for any example.

Remark 7.10. As noted in Claim 2 above, Euclid's algorithm shows that the GCD of two positive integers a and b doesn't just have the property that any common divisor c of a and b satisfies $c \leq d$, but in fact $c \mid d$. This fact also follows immediately from FTA itself. We've all learned FTA in school but, as we show here, it requires Euclid's algorithm for its proof.

Remark 7.11. Similarly, once one knows that FTA is true, an alternative method for finding GCD of two given inputs is simply to completely factorise both and pluck out the common prime factors. For example,

$$1368 = 2^3 \cdot 3^2 \cdot 19, \quad 750 = 2 \cdot 3 \cdot 5^3 \quad \Rightarrow \quad \text{GCD}(1368,\, 750) = 2 \cdot 3 = 6.$$

The disadvantage with this approach is that *Integer Factorisation* is a notorious example of a problem whch appears to be *algorithmically difficult*. In fact, for generic large inputs $a,\ b$, Euclid's algorithm runs much faster than any known factorisation algorithm (see Homework 2).

Linear Diophantine Equations. A Diophantine equation is a polynomial equation with integer coefficients, but where only integer solutions are considered valid. The study of Diophantine equations is one of the major subjects in number theory. The equation is *linear* if every variable "appears to the first degree", which is the same thing as saying that, geometrically, the equation represents a hyperplane in Euclidean space (see Remarks 7.14 and 7.15 below). Euclid's algorithm, via Bezout's lemma, leads easily to a complete theory of linear Diophantine equations, as we now show.

First consider a linear Diophantine equation in one variable. It must read $ax = b$, where a and b are integers. Clearly, it has an integer solution if and only if $a \mid b$, in which case the solution is unique, namely $x = b/a$. So far, so trivial. The important case is that of two variables.

Theorem 7.12. *Let $a,\ b,\ c \in \mathbb{Z}$. Then the Diophantine equation*

$$ax + by = c \tag{7.5}$$

either has no solution or has infinitely many. The latter occurs if and only if $d \,|\, c$, where $d = GCD(a, b)$. In that case, if $x_0,\ y_0$ are any integers satisfying $ax_0 + by_0 = d$ and $c = md$, then the general solution of (7.5) is given by

$$\begin{aligned} x &= mx_0 + \left(\frac{b}{d}\right)\, n, \\ y &= my_0 - \left(\frac{a}{d}\right)\, n, \quad n \in \mathbb{Z}. \end{aligned} \tag{7.6}$$

PROOF: Firstly, since $d \,|\, a$ and $d \,|\, b$, d will also divide any integer linear combination $ax + by$. Hence d must divide c, if (7.5) is to have a solution.

Secondly, we know by Proposition 7.8 that there exist integers $x_0,\ y_0$ satisfying $ax_0 + by_0 = d$. If $c = md$ then by direct insertion into (7.5) we see that any pair $(x,\ y)$ given by (7.6) will also satisfy (7.5). So it remains to show that (7.5) has no further solutions.

So let $(x_0,\ y_0) \in \mathbb{Z}^2$ be any pair satisfying $ax_0 + by_0 = d$ and let $(x,\ y)$ be any integer solution to (7.5). Thus

$$ax + by = c \tag{7.7}$$

and

$$a(mx_0) + b(my_0) = md = c. \tag{7.8}$$

Subtracting (7.8) from (7.7) we get

$$a(x - mx_0) = b(my_0 - y).$$

We can divide through by d to get

$$\frac{a}{d}(x - mx_0) = \frac{b}{d}(my_0 - y). \tag{7.9}$$

Lemma 7.13. *For any integers $u,\ v,\ w$ we have*

$$u \,|\, vw \ \wedge\ GCD(u,\ v) = 1 \ \Rightarrow\ u \,|\, w.$$

The lemma follows immediately from FTA. For if u divides vw then, by FTA, it means that every prime power appearing in the unique prime factorisation of u also appears in that of vw. But if GCD$(u,\ v) = 1$ it means that the prime factorisations of u and v have nothing in common. But the prime factorisation of vw is just the concatenation of those of v and w. Hence, the entire prime factorisation of u must appear in that of w, i.e.: $u \,|\, w$, v.s.v.

Now apply Lemma 7.13 to (7.9). By definition of d we have that GCD$\left(\frac{a}{d},\ \frac{b}{d}\right) = 1$. But (7.9) says, in particular, that $\frac{b}{d}$ divides the product $\frac{a}{d}(x - mx_0)$. Hence, by Lemma 7.13, $\frac{b}{d}$ must divide $x - mx_0$. In other words, there must exist an integer n such that $x - mx_0 = n\left(\frac{b}{d}\right)$, v.s.v. Substituting this expression for x into (7.5) directly yields that also $y = my_0 - n\left(\frac{a}{d}\right)$, v.s.v.

Remark 7.14. A geometrical interpretation of Theorem 7.12 is the following. The

equation $ax + by = c$ represents a line in $\mathbb{R}^2$. The theorem says that this line intersects the integer lattice $\mathbb{Z}^2$ if and only if GCD$(a,\, b)$ divides c and, in that case, that the intersection consists of an infinite sequence of evenly spaced points.

Remark 7.15. Theorem 7.12 can be generalised to an arbitrary number of variables. Given integers $a_1,\, a_2,\, \ldots,\, a_n$ and c, it is clear that a necessary condition for the existence of an integer solution to the Diophantine equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{7.10}$$

is that GCD$(a_1,\, a_2,\, \ldots,\, a_n)$ divides c. Now, by repeated application of Euclid's algorithm (a total of $n - 1$ times), one can show that this condition is also sufficient and that the general solution then contains $n - 1$ free integer variables. See Demo-3 for a worked example in three variables. Geometrically, (7.10) represents a hyperplane in $\mathbb{R}^n$ and this hyperplane intersects $\mathbb{Z}^n$ if and only if GCD$(a_1,\, a_2,\, \ldots,\, a_n)$ divides c. In that case, the intersection is an $(n - 1)$-dimensional lattice in the hyperplane.

Remark 7.16. Non-linear Diophantine equations are ... well ... hard. In studying them, one sometimes relaxes the restriction on seeking only integer solutions to allowing rational ones. But even in one variable and degree 2, it is not trivial to show that the equation $x^2 = 2$, for example, has no rational solutions. This is the statement that $\sqrt{2}$ is an irrational number. The usual proof is the following:

Suppose $\sqrt{2}$ were rational. We can write any rational number in lowest terms, hence this would mean there existed rationals $p,\, q$ satisfying $\sqrt{2} = p/q$ and GCD$(p,\, q) = 1$. Squaring both sides we get $2 = p^2/q^2 \Rightarrow p^2 = 2q^2$. In particular, p^2 is an even number, which means p is also even. Thus $p = 2r$, for some integer r. Substituting,

$$p^2 = 2q^2 \Rightarrow (2r)^2 = 2q^2 \Rightarrow q^2 = 2r^2.$$

Hence q^2 is also even, and thus q. But now both p and q are even, contradicting that GCD$(p,\, q) = 1$.

Remark 7.17. The most famous family of Diophantine equations is

$$x^n + y^n = z^n \quad n \in \mathbb{Z}_+, \text{ fixed.}$$

$n = 1$: The equation is $x + y = z$. Clearly, it has infinitely many integer solutions and these form a 2-dimensional sublattice of $\mathbb{Z}^3$, consisting of all points $\{(x,\, y,\, x + y) \in \mathbb{Z}^3 : x,\, y \in \mathbb{Z}\}$.

$n = 2$: The equation reads $x^2 + y^2 = z^2$. Positive integer solutions $(x,\, y,\, z)$ are called *Pythagorean triples*, since Pythagoras' Theorem implies they can be made the lengths of the sides of a right-angled triangle. One Pythagorean triple is $(3,\, 4,\, 5)$. This gives rise to infinitely many more: $(3n)^2 + (4n)^2 = (5n)^2$ for any $n \in \mathbb{Z}$. A *primitive* Pythagorean triple is one for which GCD$(x,\, y,\, z) = 1$. The following theorem isn't too hard to prove, but we don't have time for it:

Theorem 7.18. *There are infinitely many primitive Pythagorean triples. In any such*

triple, z is odd and exactly one of x and y is even. WLOG, assuming y is even, the complete set of primitive Pythagorean triples is given by

$$x = b^2 - a^2, \;\; y = 2ab, \;\; z = b^2 + a^2 \quad \textit{where } 1 \leq a < b \textit{ and } \textit{GCD}(a, b) = 1.$$

$n \geq 3$: Fermat's Last Theorem, proven by Andrew Wiles in 1994, asserts that there are no integer solutions with $xyz \neq 0$.

Remark 7.19. In the case of linear Diophantine equations, Euclid's algorithm provides an efficient means of deciding whether a given equation has an integer solution or not, and for finding such a solution when one exists. A natural question to ask is whether there is *any* algorithm which can take as input an *arbitrary* Diophantine equation and, in finite time, determine whether or not the equation has an integer solution (and, in the best case, find one when they exist). This is *Hilbert's 10th Problem* and, famously, the answer is "No such algorithm exists". This was proven by Matiyasevich in 1970 and is an important result in theoretical computer science.