MA503 TA Notes

Chloe Weiers

Fall 2022

Introduction!

In this document you will find examples, explanations, and some tricks to help you succeed in this course. Everything you will find here has been asked or discussed in some form in my office hours in past semesters, so I thought it would be best to simplify my life (and yours) by compiling a working document of TA notes. There is a section for every lecture in the semester, as well as an **Appendix** with a quick guide to frequently used and confused math symbols and notation. These notes are by no means complete or comprehensive, and are not a substitute for attending lectures or coming to office hours. If something here confuses you or seems suspicious, please email me (`cweiers@stevens.edu`) and we can work it out. Also, if you have any suggestions, please let me know! I made this resource for you!

Contents

1 Lecture 1: Divisibility. GCD. Congruences.

1.1 Proof by induction

First, we review a basic mathematical proof technique, proof by induction. The idea is simple: we have a statement that we want to prove. We test a single case to confirm that the statement is indeed true. Then we assume that the statement is true up to a certain point. Finally, we show that the statement is also true one single step beyond the assumed point, using the assumption previously made. Proofs by induction thus have 3 steps:

1. **The base case:** Show that the given statement is true for some "basic" case. This is often $n = 0$ or $n = 1$, depending on the context. The value of n should be chosen so that the base case statement is not trivial.
2. **The induction hypothesis:** Assume that the given statement is true for all $n \leq N$ for some fixed value of N.
3. **The inductive step:** Now use the induction hypothesis to show that the given statement is also true for $n = N + 1$.

It's probably easiest to understand how proof by induction works with a simple example. The following is the first proof by induction I ever learned how to do.

Example 1.
Question: Using induction, prove the following equality:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Solution:

1. First, let's test our base case, $n = 1$:

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}.$$

   So the given statement holds for our base case.

2. Now assume that the given statement is true up to some $n = N$. In other words, we are assuming that

$$\sum_{i=1}^{N} i = \frac{N(N+1)}{2}$$

   for some N. *This is our induction hypothesis.*

3. Now we show that the given statement holds for $n = N + 1$. We can do this using

some algebra and our induction hypothesis:

$$\begin{aligned}
\sum_{i=1}^{N+1} i &= \sum_{i=1}^{N} i + \sum_{i=N+1}^{N+1} i && \text{(splitting the sum)} \\
&= \sum_{i=1}^{N} i + (N+1) && \text{(simplifying second sum)} \\
&= \frac{N(N+1)}{2} + (N+1) && \textbf{(by induction hypothesis)} \\
&= \frac{N(N+1)}{2} + \frac{2(N+1)}{2} \\
&= \frac{(N+1)(N+2)}{2}. && \text{(factoring by grouping)}
\end{aligned}$$

Now we can see that the given statement is satisfied for $n = N+1$, and we are done!

1.2 Congruence

This is an extremely important topic! It will be used in pretty much everything in this course, so it's best to understand it now or you will suffer later.

Let's first recall the definition from the slides:

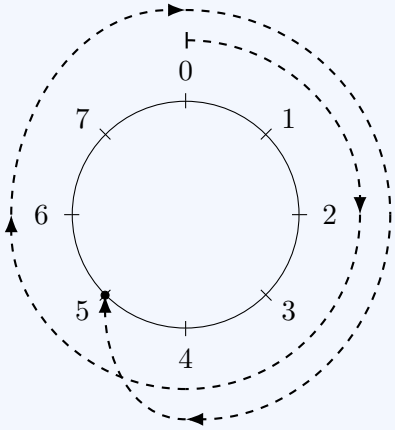
Definition 1.1. a is **congruent to** b modulo n if a and b give the same remainder when divided by n.

We use the notation $a \equiv b \bmod n$ or, more frequently, $\boldsymbol{a \equiv_n b}$. Both are read "$a$ is congruent to b mod n".

It may be useful to think about congruences in terms of a clock face with n tick marks. Consider an analog clock with 12 ticks. We don't say, "it's 25 o'clock", we say "it's 1 o'clock". That is because $25 \equiv_{12} 1$. In other words, 25/12 has remainder 1.

Example 2.
Question: What is 13 mod 8?

Solution: First, notice that 13/8 has remainder 5. Thus $\boxed{\mathbf{13 \equiv_8 5.}}$ Using a clock face with 8 ticks, we can also see that this is true by starting at 0 and counting clockwise 13 ticks:



1.2.1 Calculator trick for congruences

There is an easy way to compute congruences on your calculator. It is easiest to understand through example:

Example 3.
Question: Compute 5678 % 18.

Solution: On your calculator, do the following: type `5678-18`, hit `ENTER`. You will get `315.444444444`. Now subtract off the whole number, `315`, from the result. You will get just the decimal part, `.444444444444`. Now multiply that by the modulus, `18`. You will get `8`. That is the remainder. Your calculator screen will look something like this:

```
5678/18
          315.444444444
ANS-315
          .444444444444
ANS*18
                      8
```

You can use this to check your work or on exams. For the first few homework assignments, you are expected to show your work when calculating congruences. Another great way to check your work is using WolframAlpha (`https://www.wolframalpha.com/`). You can type the following into WolframAlpha:

```
5678 mod 18
```

Easy as that.

2 Lecture 2: Units. Euler function. CRT. RSA.

2.1 Chinese Remainder Theorem

The idea here is that we can solve systems of numerous congruences with different moduli assuming that all of the moduli are pairwise coprime. The proof of the CRT provides a kind of algorithm for solving such congruences. It is not too complicated, but it is easy to mess up the details, so be careful with your computations.

Example 4.
Question: Solve the following system of congruences:

$$\begin{aligned} x &\equiv_4 2 \\ x &\equiv_5 2 \\ x &\equiv_7 3. \end{aligned}$$

Solution: First, let's collect the information we already have (notice that $n = 4 \cdot 5 \cdot 7 = 140$):

$$\begin{array}{llll} c_1 = 2 & n_1 = 4 & m_1 = \frac{140}{4} = 35 & d_1 = ? \\ c_2 = 2 & n_2 = 5 & m_2 = \frac{140}{5} = 28 & d_2 = ? \\ c_3 = 3 & n_3 = 7 & m_3 = \frac{140}{7} = 20 & d_3 = ? \end{array}$$

Next, we need to solve for d_1, d_2, and d_3. To do so, we can simply solve the three congruences $35x \equiv_4 1$, $28x \equiv_5 1$, and $20x \equiv_7 1$ one-by-one. First, we solve for d_1:

$$\begin{aligned} 35x &\equiv_4 1 & \\ 3x &\equiv_4 1 & \text{(taking both sides mod 4)} \\ \Rightarrow x &\equiv_4 3 & \text{(since } 3 \cdot 3 = 9 \equiv_4 1\text{)}. \end{aligned}$$

Hence $d_1 = 3$. Now we solve for d_2:

$$\begin{aligned} 28x &\equiv_5 1 & \\ 3x &\equiv_5 1 & \text{(taking both sides mod 5)} \\ \Rightarrow x &\equiv_5 2 & \text{(since } 3 \cdot 2 = 6 \equiv_5 1\text{)}. \end{aligned}$$

Hence $d_2 = 2$. Now we solve for d_3:

$$\begin{aligned} 20x &\equiv_7 1 & \\ 6x &\equiv_7 1 & \text{(taking both sides mod 7)} \\ \Rightarrow x &\equiv_7 6 & \text{(since } 6 \cdot 6 = 26 \equiv_7 1\text{)}. \end{aligned}$$

Hence $d_3 = 6$. Let's restate the information that we now have:

$$\begin{array}{llll} c_1 = 2 & n_1 = 4 & m_1 = \frac{140}{4} = 35 & d_1 = \mathbf{3} \\ c_2 = 2 & n_2 = 5 & m_2 = \frac{140}{5} = 28 & d_2 = \mathbf{2} \\ c_3 = 3 & n_3 = 7 & m_3 = \frac{140}{7} = 20 & d_3 = \mathbf{6} \end{array}$$

Finally, we just need to take a linear combination of c_i's, m_i's, and d_i's to solve for x_0:

$$\begin{aligned} x_0 &= c_1 m_1 d_1 + c_2 m_2 d_2 + c_3 m_3 d_3 \\ &= (2)(35)(3) + (2)(28)(2) + (3)(20)(6) \\ &= 210 + 112 + 360 \\ &= 682 \\ &\equiv_{140} 122. \end{aligned}$$

As a sanity check, we can confirm that our solution, $x = 122$, satisfies all three original congruences, i.e.

$$\begin{aligned} 122 &\equiv_4 2 \\ 122 &\equiv_5 2 \\ 122 &\equiv_7 3. \end{aligned}$$

Indeed, it does, so $\boxed{\boldsymbol{x = 122}}$ is our solution.

2.2 Binary exponentiation

Binary exponentiation is a very useful tool for breaking down and simplifying congruences of large powers. We can see how it works through an example.

Example 5.
Question: Compute 5^{101} % 11.

Solution: First, break down 101 into a sum of powers of 2, like this:

$$101 = \underbrace{64}_{2^6} + \underbrace{32}_{2^5} + \underbrace{4}_{2^2} + \underbrace{1}_{2^0}.$$

Now we can rewrite 5^{101} as

$$5^{101} = 5^{64+32+4+1},$$

and we can solve this efficiently using the method of *successive squaring*. The idea behind this method is that we compute a large power "step-by-step" using increasingly large powers of the base. In practice, this means that at every step of the successive squaring process, the output value is bounded by the modulus, which in this case is 11. Let's see how it works:

$$\begin{aligned} 5^1 &\equiv 5 \bmod 11 \\ 5^2 = (5^1)^2 = 5^2 = 25 &\equiv 3 \bmod 11 \\ 5^4 = (5^2)^2 = 3^2 = 9 &\equiv 9 \bmod 11 \\ 5^8 = (5^4)^2 = 9^2 = 81 &\equiv 4 \bmod 11 \\ 5^{16} = (5^8)^2 = 4^2 = 16 &\equiv 5 \bmod 11 \\ 5^{32} = (5^{16})^2 = 5^2 = 25 &\equiv 3 \bmod 11 \\ 5^{64} = (5^{32})^2 = 3^2 = 9 &\equiv 9 \bmod 11. \end{aligned}$$

Notice that at each step, our result is bounded by 11. That keeps the computations manageable.
Now we recombine these powers using properties of exponents to compute 5^{101} % 11:

$$\begin{aligned} 5^{101} &= 5^{64+32+4+1} \\ &= (5^{64})(5^{32})(5^4)(5^1) \\ &= (9)(3)(9)(5) \\ &\equiv_{11} 5. \end{aligned}$$

Thus we have $\boxed{5^{101} \,\%\, 11 = 5.}$

3 Lecture 3: Primality testing. Factorization problem.

3.1 Pollard's $p-1$ algorithm

Say we have a large composite number N that is the product of two prime factors p and q, i.e. $N = pq$. The goal of Pollard's $p-1$ algorithm is to find one of these prime factors. Ideally, we want $p-1$ to have many small prime factors.[1]

Now let's review the algorithm.

Input: Large composite number N
Output: Prime factor d or "`FAILURE`"
Data: A random number a such that $\gcd(a, N) = 1$
for $n = 2, 3, \ldots$ **do**
  compute $d = \gcd(N, a^{n!} - 1)$
  if $1 < d < N$ **then**
    output d `// a nontrivial factor has been found`
  end
  else if $d = N$ **then**
    output "`FAILURE`" `// no nontrivial factor has been found`
  end
end

Algorithm 1: Pollard's $p-1$ algorithm

Note 1. Like all factorization algorithms you will learn in this class, the nice thing about this algorithm is that we can easily check our work. If the algorithm spits out some number d, just to be sure, check whether $d \mid N$. In other words, take your calculator and type in `N/d`. If the result is a whole number, great. You have found both factors of N! If not, something went wrong. You should either have a prime factor or nothing. Go back through the algorithm and see where you went wrong.

Example 6.
Question: Using Pollard's $p-1$ algorithm and $a = 2$ (starting with $n = 5$), find both nontrivial prime factors of 115147.

Solution: Here we have $N = 115147$ and $a = 2$. Since 115147 is odd, we have $\gcd(2, 115147) = 1$, so we are good. Now we start iterating through the algorithm.

1. Let $n = 2$. Now we compute, starting with $n = 5$:

$$\begin{aligned} d &= \gcd(115147, 2^{5!} - 1) \\ &= \gcd(115147, 2^{120} - 1) \\ &= 1. \end{aligned}$$

So $d = 1$, which satisfies neither $1 < d < N$ nor $d = N$, so we proceed...

[1] There is a nice, short explanation of the algorithm (with example) in [4].

2. Now we have $n = 6$:

$$\begin{aligned} d &= \gcd(115147, 2^{6!} - 1) \\ &= \gcd(115147, 2^{720} - 1) \\ &= 1. \end{aligned}$$

   No good. Onward:

3. $n = 7$:

$$\begin{aligned} d &= \gcd(115147, 2^{7!} - 1) \\ &= \gcd(115147, 2^{5040} - 1) \\ &= 113, \end{aligned}$$

   which clearly satisfies $1 < 113 < 115147$. To double check, we divide 115147 by our found factor 113, and we get

$$115147/113 = 1019.$$

So now the algorithm terminates, and we have found both nontrivial prime factors of 115147, which are **113 and 1019.**

3.2 Quadratic sieve algorithm (factorization by difference of squares)

Say we have a large composite number N that is the product of two prime numbers p and q (a familiar story). We want to factor N. The quadratic sieve algorithm works to find some numbers a and b such that $a \not\equiv_N \pm b$ and $a^2 \equiv_N b^2$. The second condition is essential, since it gives us this:

$$\begin{aligned} a^2 &\equiv_N b^2 \\ \Rightarrow a^2 - b^2 &\equiv_N 0 \quad \text{(subtracting } b^2 \text{ from both sides)} \\ \Rightarrow (a+b)(a-b) &\equiv_N 0 \quad \text{(factoring LHS)} \\ \Rightarrow \gcd(a+b, N) &\text{ or } \gcd(a-b, N) \text{ may be either } p \text{ or } q. \end{aligned}$$

So this algorithm basically uses this clever little trick to help us (sometimes) more efficiently factor N. The algorithm itself is rather complicated, so just focus on how to apply it in this class.

Here's how it's going to work: you are going to be given a large composite number N and a set of *relations*. A relation in this context is a congruence with a square of one *larger number* on one side and the *prime factorization* of that larger number on the other side (it will make sense when you look at an example). **You will be given these relations–you don't need to worry about generating them yourself.** Once you have these relations, you multiply them together in a particular way to try to find nontrivial factors of N. It's actually not so difficult in practice.

Example 7.
Question: Let $N = 299$. Use the quadratic sieve algorithm and the following relations:

$$\begin{aligned} 30^2 &\equiv_N 3 \\ 40^2 &\equiv_N 3 \cdot 5 \cdot 7 \\ 55^2 &\equiv_N 5 \cdot 7 \\ 125^2 &\equiv_N 7 \cdot 11 \end{aligned}$$

to find **both** nontrivial factors of N.

Solution: We are going to multiply together some subset of these relations until we get something of the form $a^2 \equiv_N b^2$. So we want at least **two** occurrences of each prime factor from the right-hand sides of the relations to be in our final relation. Let's multiply together the first three relations:

$$\begin{aligned} \left(30^2\right)\left(40^2\right)\left(55^2\right) &\equiv_N (3)(3 \cdot 5 \cdot 7)(5 7) \\ \left(30^2 \cdot 40^2 \cdot 55^2\right) &\equiv_N (3 \cdot 3 \cdot 5 \cdot 7 \cdot 5 \cdot 7) \\ (30 \cdot 40 \cdot 55)^2 &\equiv_N (3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7) \\ (30 \cdot 40 \cdot 55)^2 &\equiv_N \left(3^2 \cdot 5^2 \cdot 7^2\right) \\ (30 \cdot 40 \cdot 55)^2 &\equiv_N (3 \cdot 5 \cdot 7)^2. \end{aligned}$$

Ok, so now we have something of the form $a^2 \equiv_N b^2$, where $a = 30 \cdot 40 \cdot 55$, and $b = 3 \cdot 5 \cdot 7$. Let's simplify this a few steps further:

$$\begin{aligned} (30 \cdot 40 \cdot 55)^2 &\equiv_N (3 \cdot 5 \cdot 7)^2 \\ (66000)^2 &\equiv_N (3 \cdot 5 \cdot 7)^2 \quad \text{(multiplying out LHS)} \\ (220)^2 &\equiv_N (3 \cdot 5 \cdot 7)^2 \quad \text{(mod by } N = 299 \text{ on LHS)} \\ (220)^2 &\equiv_N (105)^2 \quad \text{(multiplying out RHS)} \end{aligned}$$

So now we have $a = 220$, $b = 105$. Now we need to find $\gcd(220 \pm 105, 299)$. First, let's find $\gcd(220 + 105, 299)$[a]:

$$\gcd(220 + 105, 299) = \gcd(325, 299) = 13.$$

We can see that 13 is indeed a prime factor of 299, since $299/13 = 23$. Hence the two prime factors of 299 are **13 and 123.**

[a] You can either use WolframAlpha for this (on homework) or the Euclidean algorithm (on exams). In WolframAlpha, just type `gcd(325,299)`.

3.3 Pollard's rho algorithm

The goal of Pollard's rho algorithm is identical to that of Pollard's $p-1$ algorithm–we are given a large composite number N that is the product of two primes p and q, and we want to recover one of these prime factors (the second prime factor comes for free once we get the first).

Here is the algorithm:

Input: Large composite number N, function $f(x) = x^2 + 1$
Output: Prime factor d
Data: Seed value $x_0 = 2$
for $n = 1, 2, \ldots, \lceil 2\sqrt[4]{N} \rceil$ **do**
  compute $x_n = x_{n-1}^2 + 1 \bmod N$
end
for $i = 1, 2, \ldots$ **do**
  compute $d = \gcd(x_{2i} - x_i, N)$
  if $d > 1$ **then**
    output d // a nontrivial factor has been found
  end
end

Algorithm 2: Pollard's ρ algorithm

Let's see an example.

Example 8.
Question: Using Pollard's rho algorithm, find both nontrivial factors of 1751.

Solution: Our large composite number N is 1751. Notice that $\lceil 2\sqrt[4]{1751} \rceil = 13$, so we will need to first find $x_1, \ldots, x_{13}$. Recall that we have $x_0 = 2$, which we will use to recursively calculate x_i values.

$x_0 = \mathbf{2}$ $\quad x_1 = 2^2 + 1 \equiv_N \mathbf{5}$ $\quad x_2 = 5^2 + 1 \equiv_N \mathbf{26}$
$x_3 = 26^2 + 1 \equiv_N \mathbf{677}$ $\quad x_4 = 677^2 + 1 \equiv_N \mathbf{1319}$ $\quad x_5 = 1319^2 + 1 \equiv_N \mathbf{1019}$
$x_6 = 1019^2 + 1 \equiv_N \mathbf{19}$ $\quad x_7 = 19^2 + 1 \equiv_N \mathbf{362}$ $\quad x_8 = 362^2 + 1 \equiv_N \mathbf{1471}$
$x_9 = 1471^1 + 1 \equiv_N \mathbf{1357}$ $\quad x_{10} = 1357^2 + 1 \equiv_N \mathbf{1149}$ $\quad x_{11} = 1149^2 + 1 \equiv_N \mathbf{1699}$
$x_{12} = 1699^2 + 1 \equiv_N \mathbf{954}$ $\quad x_{13} = 954^2 + 1 \equiv_N \mathbf{1348}$

Now we calculate gcds. Per the algorithm, we only need to calculate gcds of differences of the form $x_{2i} - x_i$. We start with $i = 1$ and work our way up.

$\gcd(x_2 - x_1, 1751) = \gcd(26 - 5, 1751) = 1$
$\gcd(x_4 - x_2, 1751) = \gcd(1319 - 26, 1751) = 1$
$\gcd(x_6 - x_3, 1751) = \gcd(19 - 1319, 1751) = \gcd(451, 1751) = 1$ **(remember:** mod1751**)**
$\gcd(x_8 - x_4, 1751) = \gcd(1471 - 1319, 1751) = 1$
$\gcd(x_{10} - x_5, 1751) = \gcd(1149 - 1019, 1751) = 1$
$\gcd(x_{12} - x_6, 1751) = \gcd(954 - 19, 1751) = 17.$

Finally, we have found a nontrivial factor of N, $d = 17$. Now the other factor comes for free, since we can quickly see that

$$1751/17 = 103.$$

So we have found both nontrivial prime factors of 1751, which are **17 and 103.**

4 Lecture 4: Groups. Primitive elements.

There is a lot of material in this lecture that may be more abstract than you are used to seeing. A big hangup for many students is the notation and the vocabulary, so it may be helpful for you to review some symbols before you try to do the homework. The following is just a small subset of **Appendix A**[2].

Symbol	Meaning
φ	usually indicates a *mapping*
$\to$	*general* mapping from domain to range
$\mapsto$	*specific* mapping from elements in domain to their images in range
$\times$	Cartesian product
$\mathbb{Z}$	the set of all integers
$\mathbb{N}$	the set of all natural numbers
$\mathbb{Q}$	the set of all rational numbers
$\mathbb{R}$	the set of all real numbers
$\mathbb{C}$	the set of all complex numbers
$\mathbb{Z}_n$	the set of integers modulo n
U_n	the set of units modulo n

So, if you see something like this:

$$\varphi\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},$$

it means φ is a mapping that takes elements from $\mathbb{Z}\times\mathbb{Z}$ and sends them to elements in $\mathbb{Z}$ (recall that $\mathbb{Z}\times\mathbb{Z}$ is the set of pairs of elements (a,b) where a and b are both integers). It is a *general* mapping.

Now to the main topic: groups! Groups are algebraic structures that, in a way, quantify symmetry. In short, a group is some set of elements G equipped with some sort of operation, often denoted by $\cdot$ or $+$. This operation relates the elements of G to each other in a particular way, and it must satisfy certain properties. If the operation does not satisfy those properties, the structure is not a group. Let's review the more formal definition of a group from the slides.

Definition 4.1. Let G be a set and $\cdot$ be a binary operation on G. The pair $(G,\cdot)$ is called a **group** if:

(G1) There exists $e\in G$ such that $eg=ge=g$ for every $g\in G$. The element e is called the **identity element** of G.

(G2) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ for every $a,b,c\in G$.

(G3) For every $a\in G$, there exists an element $b\in G$ such that $ab=ba=e$. This element b is called the **inverse** of a and is denoted by a^{-1}.

[2]You can find the full list (with examples) in **Appendix A** at the end of this document.

(G1), (G2), and (G3) are the *group axioms*. The first group axiom (G1) refers to *existence of unique identity*, (G2) refers to *associativity*, and (G3) refers to *existence of inverses* (the order of the axioms is not important). To prove that a given structure is a group, you need to prove that it satisfies these three axioms, and that it is closed under operation (i.e. for any a and b in the group, $a \cdot b$ is also in the group). Many groups that we work with in this class are **abelian groups**, which means that, for any two elements a and b in the group, $ab = ba$. This means that elements commute.[3]

[3]What is purple and commutes? An abelian grape.

5 Lecture 5: DLP. DH. ElGamal. Algorithms for DLP.

5.1 Discrete logarithms and the DLP

The focus of this lecture is the discrete logarithm problem and (some of) its applications in cryptography. As such it is very important for you to understand exactly what the discrete logarithm is and how to use it. Let's look at the definition from the slides.

Definition 5.1. For a fixed modulus $n \in \mathbb{N}$ and some elements $g, h \in U_n$, $x \in \mathbb{Z}$ is the *discrete logarithm of h to the base g modulo n* if $g^x \ \% \ n = h$.

Discrete logarithms are, as you may have guessed, very similar to the standard real-valued logarithms you may have learned in high school. In this class, we are only concerned with the discrete log. Let's look at a simple example before we get to some cryptosystems.

Example 9.
Question: What is $\log_7(15)$ modulo 41?

Solution: Here we have $n = 41$ (our modulus), $g = 7$ (our base), and $h = 15$. We need to find the value of x such that $7^x \equiv_{41} 15$. We can do this by enumerating powers of 7 mod 41:

$$\begin{aligned} 7^0 &\equiv_{41} 1 \\ 7^1 &\equiv_{41} 7 \\ 7^2 = 49 &\equiv_{41} 8 \\ 7^3 = 7 \cdot 8 = 56 &\equiv_{41} 15. \end{aligned}$$

We can stop calculating powers of 7 now, since we have found that $7^3 \equiv_{41} 15$. Thus $\boxed{\log_7(15) \bmod 41 = 3.}$

We can check our work by entering the following into WolframAlpha:

```
MultiplicativeOrder[7,41,15]
```

You may have guessed by now that the *discrete log problem (DLP)* is the algorithmic problem of finding the value of a discrete log like we just did. In practice, for large moduli, it is computationally intractable (as far as we know) to calculate discrete logs. This is why the DLP can be used in public-key cryptosystems such as those discussed in class.

Remark 1. Remember these two important discrete log rules:

$$\begin{aligned} \log_g(ab) &= \log_g(a) + \log_g(b) \\ \log_g(a^z) &= z \log_g(a). \end{aligned}$$

These will help you!

5.2 Pohlig-Hellman algorithm

The Pohlig-Hellman algorithm is one nice (better than brute force) way to compute discrete logs in certain classes of finite abelian (commutative) groups. Let's review the algorithm itself.

Input: Modulus n, two elements $g, h \in \mathbb{Z}_n$
Output: $x = \log_g(h) \bmod n$

compute $|g| = N = p_1^{a_1} \cdots p_k^{a_k}$
for $i = 1, \ldots, k$ **do**
  compute $N_i = \frac{N}{p_i^{a_i}}$, $g_i = g^{N_i}$, $h_i = h^{N_i}$
  compute $x_i = \log_{g_i}(h_i)$
end
use CRT to solve the following obtained system for x:

$$\begin{aligned} x &\equiv_{p_1^{a_1}} x_1 \\ &\vdots \\ x &\equiv_{p_k^{a_k}} x_k \end{aligned}$$

Algorithm 3: Pohlig-Hellman algorithm

Now an example.

Example 10.
Question: Use the Pohlig-Hellman algorithm to find $\log_6(11)$ modulo 41.

Solution: Here we have $n = 41$, $g = 6$, and $h = 11$. The first step is to compute the order of 6 modulo 41. Using WolframAlpha (or direct enumeration, or some other method of your choice), we know that $|6| = 40 = N$. Now we need to the find the prime factorization of 40, which is $40 = 2^3 \cdot 5$. Thus $p_1^{a_1} = 2^3$ and $p_2^{a_2} = 5^1$. Since $k = 2$, we only need to compute N_1, N_2, g_1, g_2, h_1, and h_2. First, let's find N_1, g_1, and h_1:

$$N_1 = \frac{40}{2^3} = \frac{40}{8} = 5, \qquad g_1 = 6^5 \equiv_{41} 27, \qquad h_1 = 11^5 \equiv_{41} 3.$$

Now N_2, g_2, and h_2:

$$N_2 = \frac{40}{5^1} = \frac{40}{5} = 8, \qquad g_1 = 6^8 \equiv_{41} = 10, \qquad h_1 = 11^8 \equiv_{41} 16.$$

Next, we need to compute x_1 and x_2.

$$\begin{aligned} x_1 &= \log_{27}(3) \\ x_2 &= \log_{10}(16). \end{aligned}$$

We can first find x_1 by enumerating powers of 27:

$$\begin{aligned} 27^0 &\equiv_{41} 1 \\ 27^1 &\equiv_{41} 27 \\ 27^2 = 27 \cdot 27 = 729 &\equiv_{41} 32 \\ 27^3 = 32 \cdot 27 = 864 &\equiv_{41} 3. \end{aligned}$$

We can stop here, since we have $27^3 \equiv_{41} 3$, so $\boldsymbol{x_1 = \log_{27}(3) = 3}$. Now for x_2:

$$\begin{aligned} 10^0 &\equiv_{41} 1 \\ 10^1 &\equiv_{41} 10 \\ 10^2 = 10 \cdot 10 = 100 &\equiv_{41} 18 \\ 10^3 = 18 \cdot 10 = 180 &\equiv_{41} 16. \end{aligned}$$

Once again we can stop, since we have $10^3 \equiv_{41} 16$, so $\boldsymbol{x_2 = \log_{10}(16) = 3}$. Now all that's left to do is solve the following system of congruences:

$$\begin{array}{l} x \equiv_{2^3} 3 \\ x \equiv_{5^1} 3 \end{array} \longrightarrow \begin{array}{l} x \equiv_8 3 \\ x \equiv_5 3 \end{array} \Rightarrow x = 3.$$

We can easily observe that $x = 3$ without even doing a single iota of work. We just use the eyeball method: look at the congruences, see that the answer is already there.
So now we're done! We can check our work by confirming that, indeed, $6^3 \equiv_{41} 11$. Thus $\boxed{\log_6(11) \text{ modulo } 41 = 3.}$

5.3 Index calculus method

The index calculus method, as the name would suggest, uses index calculus to somewhat efficiently (better than brute force) compute discrete logs. You will be given a modulus, a base, and potentially some additional constraints (such as a value of B for B-smoothness). With this given information, you will either need to calculate or will be given some relations (a bunch of congruences) that you will use to find some discrete logs. In the following example, the relations have already been generated for you; you just need to use them to calculate the specified discrete logs.

Example 11.
Question: $g = 11$ is a primitive root of $N = 47$. Use the index calculus method to compute $\log_{11}(2)$, $\log_{11}(3)$, and $\log_{11}(5)$ using the following provided powers of 11 only:

$$\begin{aligned} 11^2 &\equiv_{47} 27 \\ 11^3 &\equiv_{47} 15 \\ 11^{29} &\equiv_{47} 10. \end{aligned}$$

Solution: First, note that 47 is prime. We are told here that 11 is a primitive root of 47. That means that 11 has multiplicative order $47 - 1 = 46$, i.e. $11^{46} \equiv_{47} 1$.
Now, we are asked to calculate several discrete logs, all of base 11. We are given three congruences, all of powers of 11. So the first step here is to take $\log_{11}$ of both sides of the three congruences. This will give us

$$\begin{array}{l} \log_{11}\left(11^2\right) \equiv_{46} \log_{11}(27) \\ \log_{11}\left(11^3\right) \equiv_{46} \log_{11}(15) \\ \log_{11}\left(11^{29}\right) \equiv_{46} \log_{11}(10) \end{array} \longrightarrow \begin{array}{l} 2 \equiv_{46} \log_{11}(27) \\ 3 \equiv_{46} \log_{11}(15) \\ 29 \equiv_{46} \log_{11}(10). \end{array}$$

Notice that the modulus is now $|47| = 46$!

We can simplify the RHS of these three congruences using the helpful properties of logs–to do so, we will take the prime factorizations of 27, 15, and 10:

$$\begin{array}{lll} 2 \equiv_{46} \log_{11}(27) & 2 \equiv_{46} \log_{11}(3^3) & 2 \equiv_{46} 3\log_{11}(3) \\ 3 \equiv_{46} \log_{11}(15) \longrightarrow & 3 \equiv_{46} \log_{11}(3 \cdot 5) \longrightarrow & 3 \equiv_{46} \log_{11}(3) + \log_{11}(5) \\ 29 \equiv_{46} \log_{11}(10) & 29 \equiv_{46} \log_{11}(2 \cdot 5) & 29 \equiv_{46} \log_{11}(2) + \log_{11}(5). \end{array}$$

To make this less ugly, let's denote $\log_{11}(2)$ by l_2, $\log_{11}(3)$ by l_3, and $\log_{11}(5)$ by l_5, which give us

$$\begin{aligned} 2 &\equiv_{46} 3l_3 \\ 3 &\equiv_{46} l_3 + l_5 \\ 29 &\equiv_{46} l_2 + l_5. \end{aligned}$$

Now we need to solve for l_2, l_3, and l_5. We can solve for l_3 using the first congruence. We need to multiply both sides by 3^{-1} modulo 46, which is 31[a]:

$$2 \equiv_{46} 3l_3 \quad \Rightarrow \quad 2 \cdot 31 \equiv_{46} 3 \cdot 31 l_3 \quad \Rightarrow \quad 16 \equiv_{46} l_3.$$

So we have $l_3 = 16$, which we can plug directly into the second congruence to solve for l_5:

$$3 \equiv_{46} l_3 + l_5 \overset{l_3=16}{\Rightarrow} 3 \equiv_{46} 16 + l_5 \quad \Rightarrow \quad 3 - 16 = -13 \equiv_{46} 33 \equiv_{46} l_5.$$

Now we have $l_5 = 33$, which we can plug into the third congruence to solve for l_2:

$$29 \equiv_{46} l_2 + l_5 \overset{l_5=33}{\Rightarrow} 29 \equiv_{46} l_2 + 33 \quad \Rightarrow \quad 29 - 33 = -4 \equiv_{46} 42 \equiv_{46} l_2.$$

Now putting it all together, we have $\boxed{\log_{11}(2) = 42, \log_{11}(3) = 16, \text{ and } \log_{11}(5) = 33.}$

[a] We could also divide by 3 on both sides here, since 3 is invertible mod 46. That process would look like

$$2 \equiv_{46} 3l_3 \quad \Rightarrow \quad \frac{2}{3} \equiv_{46} l_3 \quad \Rightarrow \quad \frac{2+46}{3} = \frac{48}{3} = 16 \equiv_{46} l_3.$$

6 Lecture 6: Quadratic congruences.

6.1 Remote coin flipping protocol

This protocol was proposed in the 1980's to be used in adversarial information exchange settings in which one adversary needs to choose a number **at random** without revealing it to his/her opponent. Both participating adversaries know at every step of the protocol whether the other party is cheating, and they can prove it.[4]

Example 12.
Question: Alice sends the number $n = 209$ to Bob. Bob sends $a = 15^2 \ \% \ 209 = 16$ to Alice. What four numbers can Alice send back to Bob? Which of these numbers represent winning calls for Alice?

Solution: First, we need to find the prime factorization of $n = 209$. By trial and error (just trying to divide out increasingly large prime numbers from 209), we see that $209 = 11 \cdot 19$. Now we are given Bob's choice of random x, which is 15, and the pre-calculated value of $a = 15^2 \ \% \ 209$, which is $a = 16$. Now Alice needs to solve the quadratic congruence $x^2 \equiv_{209} 16$. Recall that there will either be 0 or 4 solutions to this quadratic congruence.
First, let's check whether there are any obvious solutions. We can immediately see that $x = \pm 4$ is a solution to the congruence, since

$$4^2 = (-4)^2 = 16 \equiv_{209} 16.$$

So we basically get those two solutions for free! Now, since we know that there are either 0 or 4 solutions, and we have already found two, there must be another two waiting to be found.
There are two ways to approach this. One is a trick and the other is a computation.
The trick (kind of a scam): We can simply notice that, in the problem statement, we were told that Bob sends $a = 15^2 \ \% \ 209 = 16$ to Alice. So we were already told (once again, for free!) that

$$15^2 = (-15)^2 \equiv_{209} 16,$$

so ± 15 are the other two solutions.
The hard way: I prefer the hard way, since I tend to not be very observant. Thankfully, the hard way is not even so hard here. First, we need to solve the following congruences one at a time:

$$\begin{cases} x^2 \equiv_{11} 16 \equiv_{11} 5 \\ x^2 \equiv_{19} 16. \end{cases}$$

First, let's solve $x^2 \equiv_{11} 5$. As always, there are many ways to solve this. We can use the properties from the slides. We have a congruence of the form $x^2 \equiv_p a$, where $p = 11$ is prime and $a = 5$ is a unit mod 11. We have $p \equiv_4 3$, so

$$x = \pm 5^{(11+1)/4} = \pm 5^{12/4} = \pm 5^3 = \pm 125 \equiv_{11} \pm 4.$$

[4] "Alice and Bob want to flip a coin by telephone. (They have just divorced, live in different cities, want to decide who gets the car.) Bob would like not to tell Alice HEADS and hear Alice (at the other end of the line) say 'Here goes... I'm flipping the coin.... You lost!' " [1]

As a sanity check, we can make sure that $4^2 \equiv_{11} 5$, which it does.
Now we solve $x^2 \equiv_{19} 16$. As above, we can immediately notice that $x = \pm 4$ satisfy this congruence, since

$$4^2 = (-4)^2 = 16 \equiv_{19} 16.$$

Now what remains is to solve the following four systems of congruences:

$$\underbrace{\begin{matrix} x \equiv_{11} 4 \\ x \equiv_{19} 4 \end{matrix}}_{x=4} \quad \underbrace{\begin{matrix} x \equiv_{11} -4 \\ x \equiv_{19} 4 \end{matrix}}_{x=-15} \quad \underbrace{\begin{matrix} x \equiv_{11} 4 \\ x \equiv_{19} -4 \end{matrix}}_{x=15} \quad \underbrace{\begin{matrix} x \equiv_{11} -4 \\ x \equiv_{19} -4 \end{matrix}}_{x=-4}$$

So the four numbers that Alice can send to Bob are $\boxed{\pm 4 \text{ and } \pm 15.}$
Now! We need to determine which of these numbers are *winning calls* for Alice. The original number that Bob chose was 15. So $\boxed{\pm 15}$ are winning calls for Alice.

6.2 Goldwasser-Micali cryptosystem

Unlike most of the cryptosystems previously discussed in this class, the security of Goldwasser-Micali cryptosystem depends on the intractability of solving the quadratic reduosity problem for a modulus of the form $N = pq$, where p and q are large primes. In other words, given a modulus $N = pq$ and an integer x, it is believed to be hard to determine whether $x = y^2 \bmod N$ for some y.
Encryption is fairly straightforward, so let's jump right to a decryption example.

Example 13.
Question: Alice's public key is $N = 187$ and $a = 7$. Bob encrypts three bits and sends Alice the ciphertext blocks

$$\boxed{185}, \boxed{15}, \text{ and } \boxed{61}.$$

Decrypt Bob's message.

Solution: First, we need to compute the prime factorization of $N = 187$. By trial and error (brute force search), we can quickly determine that $N = 11 \cdot 17$. Now we need to compute $\left(\frac{185}{11}\right)$, $\left(\frac{15}{11}\right)$, and $\left(\frac{61}{11}\right)$ (we could also compute $\left(\frac{185}{17}\right)$, $\left(\frac{15}{17}\right)$, and $\left(\frac{61}{17}\right)$, since we get the same decryption either way).

$$\left(\frac{185}{11}\right) \overset{185 \equiv_{11} 9}{=} \left(\frac{9}{11}\right) = \left(\frac{3^2}{11}\right) = \boxed{1}$$

$$\left(\frac{15}{11}\right) \overset{15 \equiv_{11} 4}{=} \left(\frac{4}{11}\right) = \left(\frac{2^2}{11}\right) = \boxed{1}$$

$$\left(\frac{61}{11}\right) \overset{61 \equiv_{1} 16}{=} \left(\frac{6}{11}\right) = \left(\frac{3}{11}\right)\left(\frac{2}{11}\right) \overset{11 \equiv_{8} 3}{=} \left(\frac{3}{11}\right)(-1)^{\frac{3 \equiv_4 3}{=}} - \left(\frac{11}{3}\right)(-1)^{\frac{11 \equiv_3 2}{=}} \left(\frac{2}{3}\right) \overset{3 \equiv_8 3}{=} \boxed{-1}.$$

Thus the message is $\boxed{001.}$

You can check your calculations of the Legendre symbols by entering the following into WolframAlpha:

```
LegendreSymbol[185, 11]
```

7 Lecture 7: Abelian groups.

7.1 Smith normal form

This is one of things that students most commonly mess up in this class. There are some strict rules about the matrix operations that you *can* and *cannot* do when you are dealing with an integer-valued matrix. You are allowed to perform *elementary row and column operations* to get a matrix into Smith normal form (SNF). In this class, we will be dealing with **integer-valued matrices**. That means that you will be given a matrix whose entries are all integers, possibly from some set $\mathbb{Z}_n$. In the past (linear algebra, differential equations), you probably learned how to perform operations on **real-valued matrices**, so there were different rules then.

!SNF mistake!

This is probably the most commonly made mistake in this class: Division is ILLEGAL! Don't do it! Matrix entries need to be integers! Even if you can divide and get an integer, DON'T DO IT! It's a trap!

Example 14.
Question: Put the following matrix with entries in $\mathbb{Z}$ into SNF (denote rows by x_1, x_2, x_3, x_4 and columns by y_1, y_2, y_3):

$$\begin{pmatrix} 1 & 4 & 7 \\ -1 & 6 & 1 \\ 0 & 5 & 1 \\ 2 & 3 & 0 \end{pmatrix}.$$

Solution: We will apply elementary row and column operations to get the given matrix into SNF. We certainly won't be doing any division, since that would cause big problems.

$$\begin{pmatrix} 1 & 4 & 7 \\ -1 & 6 & 1 \\ 0 & 5 & 1 \\ 2 & 3 & 0 \end{pmatrix} \overset{y_2 \leftarrow y_1 + y_2}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 10 & 8 \\ 0 & 5 & 1 \\ 2 & 3 & 0 \end{pmatrix} \overset{y_4 \leftarrow y_4 - 2y_1}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 10 & 8 \\ 0 & 5 & 1 \\ 0 & -5 & -14 \end{pmatrix}$$

$$\overset{y_4 \leftarrow y_3 + y_4}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 10 & 8 \\ 0 & 5 & 1 \\ 0 & 0 & -13 \end{pmatrix} \overset{y_2 \leftarrow y_2 - 2y_3}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 0 & 6 \\ 0 & 5 & 1 \\ 0 & 0 & -13 \end{pmatrix} \overset{y_4 \leftarrow y_4 + 2y_2}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 0 & 6 \\ 0 & 5 & 1 \\ 0 & 0 & -1 \end{pmatrix}$$

$$\overset{y_2 \leftarrow y_2 + 6y_4}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 0 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & -1 \end{pmatrix} \overset{y_4 \leftarrow (-1)y_4}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 0 & 0 \\ 0 & 5 & 1 \\ 0 & 0 & 1 \end{pmatrix} \overset{y_3 \leftarrow y_3 - y_4}{\rightarrow} \begin{pmatrix} 1 & 4 & 7 \\ 0 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\overset{y_1 \leftarrow y_1 - 7y_4}{\rightarrow} \begin{pmatrix} 1 & 4 & 0 \\ 0 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{x_2 \leftarrow x_2 - 4x_1}{\rightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{\text{permute rows}}{\rightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\overset{x_2\leftrightarrow x_3}{\rightarrow}\begin{pmatrix}1&0&0\\0&0&5\\0&1&0\\0&0&0\end{pmatrix}\overset{y_2\leftrightarrow y_3}{\rightarrow}\begin{pmatrix}1&0&0\\0&1&0\\0&0&5\\0&0&0\end{pmatrix}.$$

Now our matrix is in SNF.

You can check your work using Sage (Sage Cell Server online (`https://sagecell.sagemath.org/`). by entering the original matrix M, row by row, and running the following code (using matrix from previous example):

```
M = matrix([[1,4,7],[-1,6,1],[0,5,1],[2,3,0]])
M.elementary_divisors()
```

It will return the diagonal entries of the matrix in SNF. You can use this to **check your work**. If you do not show your work on your homework, you will not get points! YOU NEED TO SHOW YOUR STEPS ON HOMEWORK!! Just a friendly reminder.

7.2 Representation of finitely generated abelian groups

Before the next example, let's review a very important theorem from abstract algebra (exact statement taken from [3]).

Theorem 7.1. ***(Fundamental Theorem of Finitely Generated Abelian Groups)*** *Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form*

$$\mathbb{Z}_{(p_1)^{r_1}}\times\mathbb{Z}_{(p_2)^{r_2}}\times\cdots\times\mathbb{Z}_{(p_n)^{r_n}}\times\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z},$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers.

We will use this theorem in the following example. Don't be intimidated by it–you will only be asked to use it in applications in this class. The next example should make it clear how you will be expected to do that.

Example 15.
Question: Suppose that G is an abelian group generated by elements g_1, g_2, and g_3. Suppose also that G is subject to the following relations:

$$r_1 = 9g_1 + 1g_2 - 2g_3$$
$$r_2 = 2g_1 + 8g_2 + 4g_3.$$

We are told that this set of relations is complete. Use these relations to express G as the direct product of cyclic groups.

Solution: This may seem complicated, but it's actually very simple. All we need to do is construct a coefficient matrix from the given relations and then put that coefficient matrix into SNF. Once we have the SNF matrix, we can pull the diagonal entries to

construct the direct product of cyclic groups.
First, let's construct a coefficient matrix from the relations and put that matrix in SNF (rows are denoted by y_1, y_2 and columns by x_1, x_2, x_3):

$$\begin{pmatrix} 9 & 1 & -2 \\ 2 & 8 & 4 \end{pmatrix} \overset{y_2 \leftarrow y_2 + 2y_1}{\to} \begin{pmatrix} 9 & 1 & -2 \\ 20 & 10 & 0 \end{pmatrix} \overset{x_2 \leftarrow (-1)x_2}{\to} \begin{pmatrix} 9 & -1 & -2 \\ 20 & -10 & 0 \end{pmatrix}$$

$$\overset{x_1 \leftarrow x_1 + 2x_2}{\to} \begin{pmatrix} 7 & -1 & -2 \\ 0 & -10 & 0 \end{pmatrix} \overset{y_2 \leftarrow (-1)y_2}{\to} \begin{pmatrix} 7 & -1 & -2 \\ 0 & 10 & 0 \end{pmatrix} \overset{x_1 \leftarrow x_1 + 3x_3}{\to} \begin{pmatrix} 1 & -1 & -2 \\ 0 & 10 & 0 \end{pmatrix}$$

$$\overset{x_2 \leftarrow x_2 + x_1}{\to} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 10 & 0 \end{pmatrix} \overset{x_3 \leftarrow x_3 + 2x_1}{\to} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 10 & 0 \end{pmatrix}.$$

Now our matrix is in SNF. Thus G can be expressed as the following direct product of cyclic groups:

$$\boxed{G \simeq \mathbb{Z}_1 \times \mathbb{Z}_{10} \times \mathbb{Z}.}$$

Notice that we have an extra trailing $\mathbb{Z}$ in our direct product. You can think about it like this: the group has **three** generators, so we need **three** algebraic objects in the direct product so that all of the group dimensions are accounted for. Notice also that 10 is not prime. That is okay here. You don't need to complicate your life by rewriting and expanding things. However, if we wanted to, we could further decompose $\mathbb{Z}_{10}$ into $\mathbb{Z}_2 \times \mathbb{Z}_5$, and we would have a representation consistent with Theorem 7.1.

Remark 2. In general, for a given group G with n generators and $\alpha_1, \ldots, \alpha_m$ on the diagonal entries of the corresponding SNF matrix (obtained from a coefficient matrix of a complete set of relations), G can be expressed as a direct product of n algebraic objects like so:

$$G \simeq \underbrace{\mathbb{Z}_{\alpha_1} \times \cdots \times \mathbb{Z}_{\alpha_m} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{n}$$

In the example above, $\alpha_1 = 1$ and $\alpha_2 = 10$, so $m = 2$. Since $n = 3$, we add $n - m = 3 - 2 = 1$ additional trailing $\mathbb{Z}$.

If you have more relations than generators, you will still have n elements in the direct product–you just won't have any trailing $\mathbb{Z}$'s.

8 Lecture 8: Rings. Polynomials. Fields.

8.1 Polynomial long division

Polynomial long divison works in a very similar manner to integer long division. It may look scary, but it's really the same idea. The important thing to remember here is that we are performing operations in *fields*, usually finite fields of the form $\mathbb{Z}_p$ in this course. What this means in practice is that the coefficients in front of the variables come from a set finite field, so you will occasionally need to multiply the divisor by an element from the given field to get what you want. This is probably clearer through example.

Example 16. (From the slides)
Question: In $\mathbb{Z}_7[x]$, find the remainder of division of $f(x)$ and $g(x)$, where

$$f(x) = x^6 + 3x^5 + 4x^2 - x + 2$$
$$g(x) = x^2 + 2x - 3.$$

Solution:

$$\begin{array}{rrrrrrrl}
 & & & x^4 & +x^3 & +x^2 & +x+5 & \\
x^2+2x-3 \;\big|\; & x^6 & +3x^5 & & & +4x^2 & -x & +2 \\
 & -(x^6 & +2x^5 & -3x^4) & & \downarrow & & \textit{(mult. by } x^4\textit{)} \\
\hline
 & & x^5 & +3x^4 & & +4x^2 & & \\
 & & -(x^5 & +2x^4 & -3x^3) & & \downarrow & \textit{(mult. by } x^3\textit{)} \\
\hline
 & & & x^4 & +3x^3 & +4x^2 & -x & \\
 & & & -(x^4 & +2x^3 & -3x^2) & & \downarrow \quad \textit{(mult. by } x^2\textit{)} \\
\hline
 & & & & x^3 & +7x^2 & -x & +2 \\
 & & & & x^3 & & +6x & +2 \quad \textit{(mod 7)} \\
 & & & & -(x^3 & +2x^2 & -3x) & \textit{(mult. by } x\textit{)} \\
\hline
 & & & & & -2x^2 & +9x & +2 \\
 & & & & & 5x^2 & +2x & +2 \quad \textit{(mod 7)} \\
 & & & & & -(5x^2 & +10x & -15) \quad \textit{(mult. by 5)} \\
\hline
 & & & & & & -8x & +17 \\
 & & & & & & 6x & +3 \quad \textit{(mod 7)}
\end{array}$$

So we have:

$$f(x) = \big(x^4 + x^3 + x^2 + x + 5\big)g(x) + 6x + 3,$$

which means that

$$q(x) = x^4 + x^3 + x^2 + x + 5$$
$$r(x) = 6x + 3.$$

Thus the remainder of division is $\boxed{6x + 3.}$

We can check that our answer is correct by entering the following into WolframAlpha:

```
PolynomialMod[(x^4+x^3+x^2+x+5)*(x^2+2x-3)+(6x+3), 7]
```

And we can confirm that this indeed returns $f(x)$. In general, for division of $f(x)$ by $g(x)$ with coefficients in $\mathbb{Z}_p$ that yields $f(x) = q(x)g(x) + r(x)$, you can check your work by confirming that $f(x) =$ `PolynomialMod[q(x)*g(x)+r(x), p]` holds.

8.2 Polynomial gcd

Example 17. (From the slides)
Question: In $\mathbb{Z}_3[x]$, use the Euclidean lemma to find $\gcd(f(x), g(x))$, where

$$f(x) = x^5 + 2x^3 + x + 1$$
$$g(x) = x^4 + x + 2.$$

Solution: First, since the degree of f, 5, is greater than the degree of g, 4, we will divide f by g. Remember that we are doing calculations in $\mathbb{Z}_3$!

$$\begin{array}{rl|llll|l} & & & & & x & & \\ \hline x^4+x+2 & | & x^5 & +2x^3 & & +x & +1 & \\ & | & -(x^5 & & +x^2 & +2x) & \downarrow & \textit{(mult. by } x\textit{)} \\ \hline & | & & 2x^3 & -x^2 & -x & +1 & \\ & | & & 2x^3 & +2x^2 & +2x & +1 & \textit{(mod 3)} \end{array}$$

We now have $f(x) = xg(x) + 2x^3 + 2x^2 + 2x + 1$. We will divide $g(x)$ by the remainder $2x^3 + 2x^2 + 2x + 1$:

$$\begin{array}{rl|llll|l} & & & & & 2x & +1 & \\ \hline 2x^3+2x^2+2x+1 & | & x^4 & & & +x & +2 & \\ & | & -(x^4 & +x^3 & +x^2 & +2x) & \downarrow & \textit{(mult. by } 2x\textit{)} \\ \hline & | & & -x^3 & -x^2 & -x & +2 & \\ & | & & 2x^3 & +2x^2 & +2x & +2 & \textit{(mod 3)} \\ & | & & -(2x^3 & +2x^2 & +2x & +1) & \textit{(mult. by 1)} \\ \hline & | & & & & & 1 & \end{array}$$

This leaves us with $g(x) = (2x+1)(2x^3 + 2x^2 + 2x + 1) + 1$. Now we can use the Euclidean lemma for polynomials to find $\gcd(f(x), g(x))$:

$$\begin{aligned} f(x) = xg(x) + 2x^3 + 2x^2 + 2x + 1 \quad &\Rightarrow \quad \gcd(f(x), g(x)) = \gcd(2x^3 + 2x^2 + 2x + 1, g(x)) \\ g(x) = (2x+1)(2x^3 + 2x^2 + 2x + 1) + 1 \quad &\Rightarrow \quad = \gcd(1, 2x^3 + 2x^2 + 2x + 1) = 1. \end{aligned}$$

Thus $\boxed{\gcd(f(x), g(x)) = 1.}$

9 Lecture 9: Classification of finite fields.

As in Lecture 4, a lot of material in this lecture may seem exceedingly abstract. It's okay if you don't understand 100% of the theory. You will be asked to do some basic computational exercises with finite fields and polynomial rings. As long as you are reasonably comfortable doing such computations, you don't have too much to worry about.

As indicated in the slides, this lecture has many parallels to the very first lecture in the course. The concepts are almost identical. In the first lecture, we looked at operations with integers. In this lecture, we are looking at analogs of those same operations with certain types of polynomials in special structures.

Example 18.
Question: Let $f(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$.

(a) Prove that $E = \mathbb{Z}_2[x]/\langle f(x)\rangle$ is a field by showing that $f(x)$ is irreducible.

(b) Find $\chi(E)$, $|E|$, and $|E^*|$.

(c) Find $(x+1)^{-1}$ in E.

Solution:

(a) We need to show that $f(x)$ is irreducible. Notice that $f(x)$ is of degree 4. So to show irreducibility, we need to check both *linear* (degree 1) and irreducible *quadratic* (degree 2) factors. We do not need to worry about checking degree 3 factors, since any degree 3 factor would need to be multiplied by a degree 1 factor to yield a degree 4 polynomial.

Recall that, in $\mathbb{Z}_2[x]$, these are the irreducible linear and quadratic polynomials (from Lecture 8):

$$\longrightarrow \quad x, x+1, x^2+x+1. \quad \longleftarrow$$

To check whether x is a factor, we can simply plug in $x = 0$ to $f(x)$[a]:

$$f(0) = 0^4 + 0 + 1 = 1 \neq 0.$$

Thus x is not a factor. Now we check whether $x+1$ is a factor:

$$f(1) = 1^4 + 1 + 1 = 3 \equiv_2 1 \neq 0.$$

So $x+1$ is not a factor either. Now we need to check whether x^2+x+1 is a factor of $f(x)$. To do so, we can try dividing out x^2+x+1 from $f(x)$ and see whether we get a remainder.

$$\begin{array}{rl|lll} & & & x^2 & +x & \\ \hline x^2+x+1 & & x^4 & & +x & +1 \\ & & -(x^4 & +x^3 & +x^2) & \downarrow \quad \textit{(mult. by } x^2\textit{)} \\ \hline & & & -x^3 & -x^2 & +x \\ & & & x^3 & +x^2 & +x \quad \textit{(mod 2)} \\ \hline & & & -(x^3 & +x^2 & +x) \quad \downarrow \quad \textit{(mult. by } x\textit{)} \\ & & & & & +1 \end{array}$$

Thus 1 is the remainder of division, so x^2+x+1 is indeed *not* a factor of $f(x)$.

(b) Remember that the characteristic $\chi(E)$ is the number of times that the multiplicative identity of a field needs to be added together to get the additive identity. The multiplicative identity in this case is 1, and the additive identity is 0. Since $1+1=0$ in $\mathbb{Z}_2$, $\boxed{\chi(E)=2.}$

The degree of f is 4, thus the size of E, $|E|$, is $2^4 = \boxed{16.}$ It follows that the size of the multiplicative group of E, $|E^*|$, is $16-1=\boxed{15.}$

(c) Finally, we need to find the inverse of the element $(x+1)$ in E. We could make a multiplication table (which is a huge hassle), OR we could think like this: the inverse of any element $g(x)$ of degree 1 in E is going to be some element of the form ax^3+bx^2+cx+d such that $(ax^3+bx^2+cx+d)\cdot g(x) \equiv_{f(x)} 1$. We know that this element will be of degree 3 since our modulus is of degree 4, and we want the product of the elements (which will be of degree 4) to be equivalent to 1 $b \mod f(x)$).

So! Let's set up a system of congruences based on the following:

$$\begin{aligned}(x+1)(ax^3+bx^2+cx+d) &\equiv_{f(x)} 1\\ ax^4+bx^3+cx^2+dx+ax^3+bx^2+cx+d &\equiv_{f(x)} 1\\ ax^4+(a+b)x^3+(b+c)x^2+(c+d)x+d &\equiv_{f(x)} 1.\end{aligned}$$

Notice that we now have a polynomial of degree 4. Recall that our modulus is x^4+x+1. By definition, then, we have

$$\begin{aligned}x^4+x+1 &\equiv_{f(x)} 0\\ \Rightarrow\ x^4 &\equiv_{f(x)} -x-1\\ \Rightarrow\ x^4 &\equiv_{f(x)} x+1 \quad (mod\ 2)\end{aligned}$$

We can use this to simplify our congruences.

$$\begin{aligned}ax^4+(a+b)x^3+(b+c)x^2+(c+d)x+d &\equiv_{f(x)} 1\\ a(x+1)+(a+b)x^3+(b+c)x^2+(c+d)x+d &= 1\\ ax+a+(a+b)x^3+(b+c)x^2+(c+d)x+d &= 1\\ (a+b)x^3+(b+c)x^2+(a+c+d)x+(a+d) &= 1.\end{aligned}$$

Now we need to find a, b, c, and d, so we need to solve a system of congruences.

$$\begin{aligned}a+b &\equiv_2 0\\ b+c &\equiv_2 0\\ a+c+d &\equiv_2 0\\ a+d &\equiv_2 1.\end{aligned}$$

First, we solve for d:

$$\begin{aligned}a+b \equiv_2 0 \ &\Rightarrow\ a \equiv_2 b,\\ b+c \equiv_2 0 \ &\Rightarrow\ b \equiv_2 c \ \Rightarrow\ a \equiv_2 b \equiv_2 c,\end{aligned}$$

so

$$a+c+d \equiv_2 0 \;\Rightarrow\; 2a+d \equiv_2 0 \;\Rightarrow\; d \equiv_2 0.$$

Substituting back, we get $a=1$, $b=1$, $c=1$, and $d=0$, so $\boxed{(x+1)^{-1} = x^3+x^2+x}$ in E.

[a] Think about it like this: If $f(0)=0$, then $x=0$ is a factor, which means that x is a factor. If $f(1)=0$, then $x=1$ is a factor, which means that $x-1=0$ is a factor, which means that (taking mod 2) $x+1$ is a factor.

10 Lecture 10: Vector spaces. Applications.

10.1 Blakley's (t, n)-threshold scheme

As discussed in class, secret sharing is a very useful tool that, as the name suggests, allows multiple parties to share a secret in such a way that a certain number of participants are required to reconstruct the secret. Here is a nice explanation of the idea from [5].

> Suppose you and your friend accidentally discovered a map that you believe would lead you to an island full of treasure. You and your friend are very excited and would like to go home and get ready for the exciting journey to the great fortune. Now who is going to keep the map? Suppose you and your so-called friend do not really trust each other and are afraid that, if the other one has the map he/she might just go alone and take everything. Now we need a scheme that could make sure that the map is shared in a way so that no one would be left out in this trip. What would you suggest?
> An easy way to solve this problem is to split the map into two pieces and make sure that both pieces are needed in order to find the island. Now we give one piece to each. You can happily go home and be assured that your friend has to go with you in order to find the island. This illustrates the basic concept of *secret sharing*.

The concept is not so difficult in practice either.

In Blakley's (t, n)-threshold scheme, the dealer generates n random vectors with entries from a preset field F. Then, for each random vector, she computes a linear combination of the (preselected) secret with each vector and sends one resulting equation to each player. The whole idea is that any t players can reconstruct the secret. The secret is an element $(\beta_1, \ldots, \beta_t) \in F^t$ (i.e. a t-dimensional vector with entries in F). As always, let's look at an example.

Example 19.
Question: Consider an instance of the Blakley $(2, 3)$-threshold scheme in which the dealer uses the field $\mathbb{Z}_{13}$ and distributes the following shares:

$$\begin{aligned} \textbf{(\#1)} \quad & 3x_1 + 5x_2 = 9 \\ \textbf{(\# 2)} \quad & 10x_1 - x_2 = 0 \\ \textbf{(\# 3)} \quad & 5x_1 + 7x_2 = 3. \end{aligned}$$

What is the secret?

Solution: Since this is a $(2, 3)$-threshold scheme, there are 3 participants and 2 shares are required to reconstruct the secret.
All we need to do is solve the system

$$\begin{cases} 3x_1 + 5x_2 \equiv_{13} 9 \\ 10x_1 - x_2 \equiv_{13} 0 \\ 5x_1 + 7x_2 \equiv_{13} 12. \end{cases}$$

First, let's solve for x_1 and x_2. Looking at the second congruence, we can immediately see

that

$$10x_1 - x_2 \equiv_{13} 0 \quad \Rightarrow \quad x_2 \equiv_{13} 10x_1.$$

Now, substituting back $x_2 \equiv_{13} 10x_1$ into the first and last congruences, we get the system

$$\begin{cases} 3x_1 + 5(10x_1) \equiv_{13} 9 \\ 5x_1 + 7(10x_1) \equiv_{13} 12 \end{cases} \Rightarrow \begin{cases} 53x_1 \equiv_{13} 9 \\ 75x_1 \equiv_{13} 12 \end{cases} \overset{\text{mod } 13}{\Rightarrow} \begin{cases} x_1 \equiv_{13} 9 \\ 10x_1 \equiv_{13} 12. \end{cases}$$

We can immediately see that $x_1 = 9$ is a solution to both congruences. Thus $x_2 = 10 \cdot 9 = 90 \equiv_{13} 12$. Thus the secret is $\boxed{(x_1, x_2) = (9, 12).}$

10.2 Shamir's (t, n)-threshold scheme

The idea behind Shamir's (t, n)-threshold scheme is very similar to Blakley's threshold scheme–a trusted dealer generates $t - 1$ random elements from a fixed field F, computes some polynomial with those random elements as coeffiients, and then generates and distributes some n values to the participants using that polynomial. At least t shares are required to reconstruct the secret. The secret is reconstructed using a Lagrange polynomial. Let's take a look.

Example 20.
Question: Consider an instance of Shamir's $(3, 3)$-threshold scheme over $\mathbb{Z}_5$ in which the dealer distributes the following shares:

$$\begin{aligned} &\textbf{(\#1)} \quad (3, f(3)) = (3, 2), \\ &\textbf{(\#2)} \quad (1, f(1)) = (1, 1), \\ &\textbf{(\#3)} \quad (4, f(4)) = (4, 1). \end{aligned}$$

What is the secret?

Solution: Here, we have a $(3, 3)$-threshold scheme, which means that there are 3 participants and all 3 shares are required to reconstruct the secret. So we first need to compute three Lagrange polynomials (one from each share), and then use values obtained from those polynomials to reconstruct the secret.
The first Lagrange polynomial, $l_1(x)$, can be constructed according the interpolation formula from the slides:

$$l_1(x) = \left(\frac{x - x_2}{x_1 - x_2}\right)\left(\frac{x - x_3}{x_1 - x_3}\right) = \frac{(x-1)(x-4)}{(3-1)(3-4)}$$

$$= \frac{x^2 - 5x + 4}{(-2)} \overset{\text{mod } 5}{=} \frac{x^2 + 4}{3} \overset{3^{-1}=2}{=} 2x^2 + 8 \overset{\text{mod } 5}{=} \mathbf{2x^2 + 3.}$$

The second Lagrange polynomial can be constructed as above.

$$l_2(x) = \left(\frac{x - x_1}{x_2 - x_1}\right)\left(\frac{x - x_3}{x_2 - x_3}\right) = \frac{(x-3)(x-4)}{(1-3)(1-4)}$$

$$= \frac{x^2 - 7x + 12}{6} \overset{\text{mod } 5}{=} \frac{x^2 + 3x + 2}{1} = \mathbf{x^2 + 3x + 2.}$$

And, finally, the third polynomial:

$$l_3(x) = \left(\frac{x-x_1}{x_3-x_1}\right)\left(\frac{x-x_2}{x_3-x_2}\right) = \frac{(x-3)(x-1)}{(4-3)(4-1)}$$

$$= \frac{x^2-4x+3}{3} \overset{\text{mod } 5}{=} \frac{x^2+x+3}{3}$$

$$\overset{3^{-1}=2}{=} 2x^2+2x+6 \overset{\text{mod } 5}{=} \mathbf{2x^2+2x+1.}$$

Now, from the problem statement, we know that $f(3) = 2$, $f(1) = 1$, and $f(4) = 1$. We can combine all of this together to get one mega polynomial $L(x)$.

$$\begin{aligned} L(x) &= 2\left(\mathbf{2x^2+3}\right) + 1\left(\mathbf{x^2+3x+2}\right) + 1\left(\mathbf{2x^2+2x+1}\right) \\ &= 4x^2+6+x^2+3x+2+2x^2+2x+1 \\ &= 7x^2+5x+9 \\ &\overset{\text{mod } 5}{=} 2x^2+4. \end{aligned}$$

So $L(x) = 2x^2+4$. Finally, the secret is simply $L(0) = 2(0)^2+4 = \boxed{\mathbf{4.}}$

11 Lecture 11: Elliptic curves.

The last two lectures in this course focus on *elliptic curves* and their applications to cryptography. Elliptic curves are simply sets of points satisfying a certain type of equation, with addition of points defined as shown on the slides. Let's review the definition.

Definition 11.1. An **elliptic curve** $\mathcal{E}$ is the set of solutions (with a special element $\mathcal{O}$) on an equation of the form

$$y^2 = x^3 + ax + b, \tag{1}$$

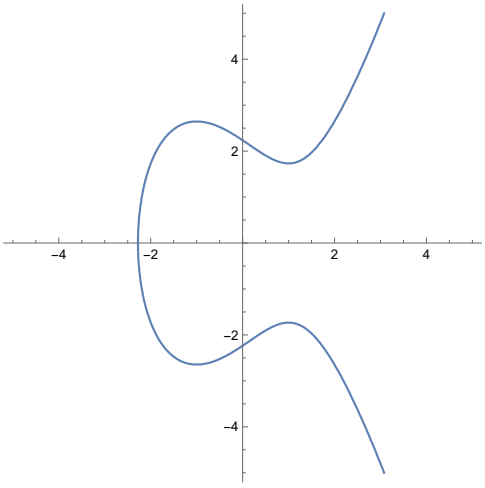
called a **Weierstrass** equation.

Addition of points on $\mathcal{E}$ is defined on the slides. The point $\mathcal{O}$ is the identity element, and is sometimes also referred to as the point at infinity.

To visualize an elliptic curve $\mathcal{E}$, you can use the following Mathematica code (using $y^2 = x^3 - 3x + 5$ as an example):

```
In[1]:= f[x_, a_, b_] := x^3 + a*x + b;
        ContourPlot[y^2 == f[x, -3, 5], {x, -5, 5}, {y, -5, 5},
        Axes -> True, Frame -> False]
```

Out[1]=



One of the fundamental ideas in this lecture is the idea of an *elliptic curve over a finite field*. Such curves are simply sets of points (x, y) satisfying some Weierstrass equation (1) such that each element x and y is in some predetermined finite field $\mathbb{Z}_p$. One thing to remember here is that, when we perform addition over such a curve, *arithmetic operations must be done with respect to* $\mathbb{Z}_p$.

Example 21.
Question: Find all points on the elliptic curve $\mathcal{E}$ defined by the equation

$$y^2 = x^3 + 2x + 2$$

over $\mathbb{Z}_5$. This table may help you:

Congruence	Solution
$y^2 \equiv_5 0$	$y = 0$
$y^2 \equiv_5 1$	$y = 1, 4$
$y^2 \equiv_5 2$	none
$y^2 \equiv_5 3$	none
$y^2 \equiv_5 4$	$y = 2, 3.$

Solution: We are given a Weierstrass equation with values $a = 2$ and $b = 2$ over the field $\mathbb{Z}_5$. All we need to do to find points on the curve is plug in values from $\mathbb{Z}_5$ for x and see whether there are solutions to the resulting quadratic congruence.
$\rightarrow$ First, $\mathcal{O}$ is on $\mathcal{E}$. We get that for free (since $\mathcal{O}$ is the identity).
$\rightarrow$ Next, let's plug in $x = 0$.

$$y^2 = (0)^3 + 2(0) + 2$$
$$y^2 = 2.$$

Are there solutions to $y^2 = 2$ in $\mathbb{Z}_5$? Looking at the table above, we can see that there are no solutions to $y^2 \equiv_5 2$, so $x = 0$ does not produce any points on $\mathcal{E}$.
$\rightarrow$ Now, $x = 1$:

$$y^2 = (1)^3 + 2(1) + 2$$
$$y^2 = 5 \equiv_5 0.$$

From the table, we can see that $y = 0$ is a solution to $y^2 \equiv_5 0$, so the point $\mathbf{(1, 0)}$ is on $\mathcal{E}$.
$\rightarrow$ $x = 2$:

$$y^2 = (2)^3 + 2(2) + 2$$
$$y^2 = 14 \equiv_5 4.$$

From the table, $y = 2, 3$ are solutions to $y^2 \equiv_5 4$, so the points $\mathbf{(2, 2)}$ and $\mathbf{(2, 3)}$ are on $\mathcal{E}$.
$\rightarrow$ $x = 3$:

$$y^2 = (3)^3 + 2(3) + 2$$
$$y^2 = 35 \equiv_5 0.$$

From the table, $y = 0$ is a solution to $y^2 \equiv_5 0$, so the point $\mathbf{(3, 0)}$ is on $\mathcal{E}$.
$\rightarrow$ Finally, $x = 4$:

$$y^2 = (4)^3 + 2(4) + 2$$
$$y^2 = 74 \equiv_5 4.$$

Once again from the table, $y = 2, 3$ are solutions to $y^2 \equiv_5 4$, so the points $\mathbf{(4, 2)}$ and $\mathbf{(4, 3)}$ are on $\mathcal{E}$.
So the set of all points on $\mathcal{E}$ is $\boxed{\mathbf{\{\mathcal{O}, (1, 0), (2, 2), (2, 3), (3, 0), (4, 2), (4, 3)\}.}}$

Below is the curve from the previous example. Notice two things: first, this is the whole curve. The curve is a finite set of points in $\mathbb{Z}_5^2$. Second, the curve has some geometric symmetry. It is worthwhile to consider where this symmetry comes from.

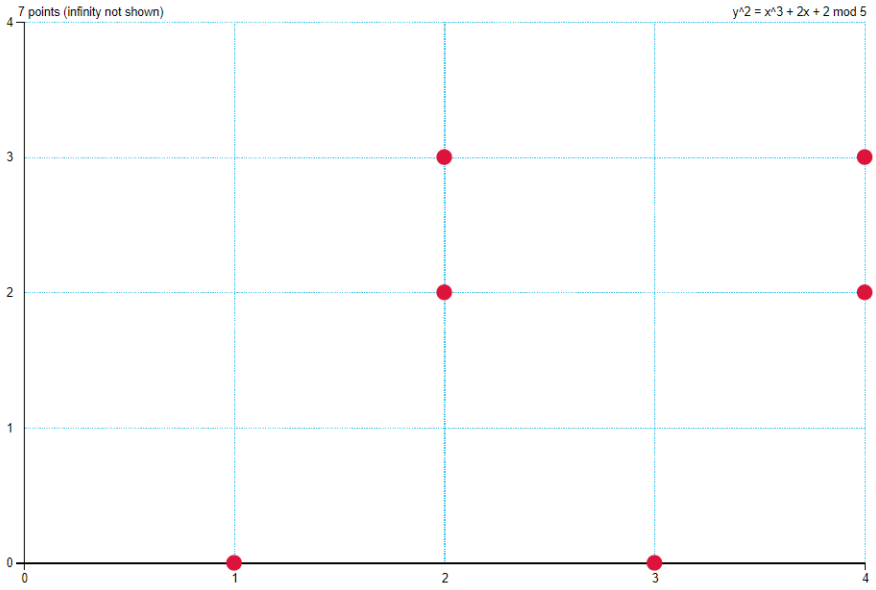


Figure 1: $y^2 = x^3 + 2x + 2$ over $\mathbb{Z}_5$ [2]

Let's now look at one more example involving adding points on an elliptic curve over a finite field.

Example 22.
Question: Consider the elliptic curve $\mathcal{E}$ defined by the equation

$$\boldsymbol{y^2 = x^3 + 2x + 5}$$

over $\mathbb{Z}_{13}$. Calculate the following:

(a) $(2,2) \oplus (3,8)$,

(b) $(4,5) \oplus (4,8)$.

Solution: We are given a Weierstrass equation with $a = 2$ and $b = 5$ over the field $\mathbb{Z}_{13}$.

(a) First, we want to find $(2,2) \oplus (3,8)$. We have $x_1 = 2$, $x_2 = 3$, $y_1 = 2$, $y_2 = 8$. Since $x_1 \neq x_2$, we use the addition formula for Case-I. First, we calculate the slope λ:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-2}{3-2} = 6.$$

Now we need to find x_3 and y_3 using the formula from the slides.

$$x_3 = \lambda^2 - x_1 - x_2 = 6^2 - 2 - 3 = 36 - 2 - 3 = 31 \equiv_{13} 5$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = 6(2-5) - 2 = 6(-3) - 3 = -20 \equiv_{13} 6.$$

Thus $(2,2) \oplus (3,8) = \boxed{(5,6).}$

(b) Now we want to find $(4,5) \oplus (4,8)$. We have $x_1 = 4$, $x_2 = 4$, $y_1 = 5$, $y_2 = 6$. Since $x_1 = x_2$ and $y_1 \neq y_2$, it is Case-IV, and thus $(4,5) \oplus (4,8) = \boxed{\mathcal{O}.}$

And, just for kicks, here is the curve from the previous example.

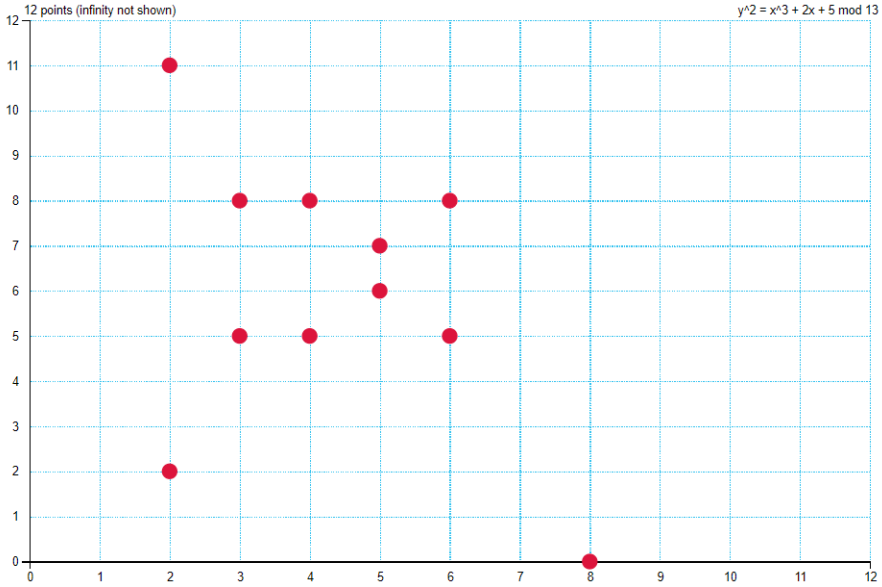


Figure 2: $y^2 = x^3 + 2x + 5$ over $\mathbb{Z}_{13}$ [2]

12 Lecture 12: ECDLP. ECC.

The discrete log problem for elliptic curves is almost identical to the discrete log problem for general groups that was discussed earlier in the course. The only difference here is that the computations are done on elements in elliptic curve groups, and thus the multiplication operation is performed using the point multiplication formulas from Lecture 11. Let's review the statement of the DLP.

Definition 12.1. The *discrete logarithm problem (DLP)* for an elliptic curve $\mathcal{E}$ is the following algorithmic problem: given $h, g \in \mathcal{E}$, find $n \in \mathbb{N}$ satisfying $h = n \cdot g$.

12.1 Elliptic curve computational Diffie-Hellman

First, let's recall the statement of the Elliptic curve computational Diffie-Hellman (ECCDH) key exchange problem for elliptic curves.

Definition 12.2. (ECCDH for an elliptic curve $\mathcal{E}$)
Given $(g, a \cdot g, b \cdot g)$, compute $(ab) \cdot g$.

In this course, you will be given an instance of ECCDH in the form $(g, a \cdot g, b \cdot g)$, and you will be asked to *solve* that instance. To solve such an instance, you need to compute the shared key $(ab) \cdot g$ as the protocol states.

Example 23.
Question: Consider the elliptic curve $\mathcal{E}$ defined by the equation

$$y^2 = x^3 + 2x + 5$$

over $\mathbb{Z}_{13}$. Solve an instance $((2,2),(3,5),(6,5))$ of an ECCDH. **The addition table below will help you with this.**

	$\mathcal{O}$	$(2,2)$	$(2,11)$	$(3,5)$	$(3,8)$	$(4,5)$	$(4,8)$	$(5,6)$	$(5,7)$	$(6,5)$	$(6,8)$	$(8,0)$
$\mathcal{O}$	$\mathcal{O}$	$(2,2)$	$(2,11)$	$(3,5)$	$(3,8)$	$(4,5)$	$(4,8)$	$(5,6)$	$(5,7)$	$(6,5)$	$(6,8)$	$(8,0)$
$(2,2)$	$(2,2)$	$(5,7)$	$\mathcal{O}$	$(4,5)$	$(5,6)$	$(6,5)$	$(3,8)$	$(2,11)$	$(3,5)$	$(8,0)$	$(4,8)$	$(6,8)$
$(2,11)$	$(2,11)$	$\mathcal{O}$	$(5,6)$	$(5,7)$	$(4,8)$	$(3,5)$	$(6,8)$	$(3,8)$	$(2,2)$	$(4,5)$	$(8,0)$	$(6,5)$
$(3,5)$	$(3,5)$	$(4,5)$	$(5,7)$	$(8,0)$	$\mathcal{O}$	$(6,8)$	$(2,11)$	$(2,2)$	$(6,5)$	$(4,8)$	$(5,6)$	$(3,8)$
$(3,8)$	$(3,8)$	$(5,6)$	$(4,8)$	$\mathcal{O}$	$(8,0)$	$(2,2)$	$(6,5)$	$(6,8)$	$(2,11)$	$(5,7)$	$(4,5)$	$(3,5)$
$(4,5)$	$(4,5)$	$(6,5)$	$(3,5)$	$(6,8)$	$(2,2)$	$(4,8)$	$\mathcal{O}$	$(5,7)$	$(8,0)$	$(3,8)$	$(2,11)$	$(5,6)$
$(4,8)$	$(4,8)$	$(3,8)$	$(6,8)$	$(2,11)$	$(6,5)$	$\mathcal{O}$	$(4,5)$	$(8,0)$	$(5,6)$	$(2,2)$	$(3,5)$	$(5,7)$
$(5,6)$	$(5,6)$	$(2,11)$	$(3,8)$	$(2,2)$	$(6,8)$	$(5,7)$	$(8,0)$	$(4,8)$	$\mathcal{O}$	$(3,5)$	$(6,5)$	$(4,5)$
$(5,7)$	$(5,7)$	$(3,5)$	$(2,2)$	$(6,5)$	$(2,11)$	$(8,0)$	$(5,6)$	$\mathcal{O}$	$(4,5)$	$(6,8)$	$(3,8)$	$(4,8)$
$(6,5)$	$(6,5)$	$(8,0)$	$(4,5)$	$(4,8)$	$(5,7)$	$(3,8)$	$(2,2)$	$(3,5)$	$(6,8)$	$(5,6)$	$\mathcal{O}$	$(2,11)$
$(6,8)$	$(6,8)$	$(4,8)$	$(8,0)$	$(5,6)$	$(4,5)$	$(2,11)$	$(3,5)$	$(6,5)$	$(3,8)$	$\mathcal{O}$	$(5,7)$	$(2,2)$
$(8,0)$	$(8,0)$	$(6,8)$	$(6,5)$	$(3,8)$	$(3,5)$	$(5,6)$	$(5,7)$	$(4,5)$	$(4,8)$	$(2,11)$	$(2,2)$	$\mathcal{O}$

Solution: Here is the information with which we are provided:

$$\begin{aligned} g &= (2,2) \\ a \cdot g &= (3,5) \\ b \cdot g &= (6,5), \end{aligned}$$

and our curve is defined by a Weierstrass equation with $a = 2$ and $b = 5$ over the field $\mathbb{Z}_{13}$. **All we need to do here is calculate $(ab) \cdot g$.** In order to do so, however, we first need to find a and b from the information provided.
$\rightarrow$ First, let's find a. We have $a \cdot g = (3,5)$, and since $g = (2,2)$, we need to solve

$$a \cdot (2,2) = (3,5).$$

Now we can use the table provided to determine a–we simply need to figure out how many times $(2,2)$ is multiplied by itself in order to produce $(3,5)$:

$$\begin{aligned} \mathcal{O} \cdot (2,2) &= (2,2) \\ (2,2) \cdot (2,2) &= (5,7) \\ (2,2) \cdot (2,2) \cdot (2,2) = (5,7) \cdot (2,2) &= (3,5). \end{aligned}$$

Since $3 \cdot (2,2) = (3,5)$, we have $a = 3$.
$\rightarrow$ Now we need to find b. From the problem statement, we know that $b \cdot g = (6,5)$, and $g = (2,2)$, so we need to solve

$$b \cdot (2,2) = (6,5).$$

We can use the exact same procedure as above:

$$\begin{aligned} \mathcal{O} \cdot (2,2) &= (2,2) \\ (2,2) \cdot (2,2) &= (5,7) \\ (2,2) \cdot (2,2) \cdot (2,2) = (5,7) \cdot (2,2) &= (3,5) \\ (2,2) \cdot (2,2) \cdot (2,2) \cdot (2,2) = (3,5) \cdot (2,2) &= (4,5) \\ (2,2) \cdot (2,2) \cdot (2,2) \cdot (2,2) \cdot (2,2) = (4,5) \cdot (2,2) &= (6,5). \end{aligned}$$

Since $5 \cdot (2,2) = (6,5)$, $b = 5$.
$\rightarrow$ Now all we need to do is calculate $(ab) \cdot g$.

$$(ab) \cdot g = (3 \cdot 5) \cdot (2,2) = 3 \cdot (5 \cdot (2,2)) = 3 \cdot (6,5) = (3,5).$$

So the shared key is $\boxed{(3,5).}$

12.2 Elliptic curve ElGamal PKC

Example 24.
Question: Consider the elliptic curve $\mathcal{E}$ defined by the equation

$$y^2 = x^3 + x + 5$$

over $\mathbb{Z}_{13}$. Let $g = (3, 10)$ and $A = (7, 11)$ be Alice's public key for EC-ElGamal encryption. Bob sends Alice ciphertext (c_1, c_2), where $c_1 = (12, 9)$ and $c_2 = (7, 2)$. Find Bob's message. **The addition table below will help you.**

	$\mathcal{O}$	$(3,3)$	$(3,10)$	$(7,2)$	$(7,11)$	$(10,1)$	$(10,12)$	$(12,4)$	$(12,9)$
$\mathcal{O}$	$\mathcal{O}$	$(3,3)$	$(3,10)$	$(7,2)$	$(7,11)$	$(10,1)$	$(10,12)$	$(12,4)$	$(12,9)$
$(3,3)$	$(3,3)$	$(10,12)$	$\mathcal{O}$	$(12,9)$	$(7,2)$	$(3,10)$	$(12,4)$	$(7,11)$	$(10,1)$
$(3,10)$	$(3,10)$	$\mathcal{O}$	$(10,1)$	$(7,11)$	$(12,4)$	$(12,9)$	$(3,3)$	$(10,12)$	$(7,2)$
$(7,2)$	$(7,2)$	$(12,9)$	$(7,11)$	$(3,3)$	$\mathcal{O}$	$(12,4)$	$(10,1)$	$(3,10)$	$(10,12)$
$(7,11)$	$(7,11)$	$(7,2)$	$(12,4)$	$\mathcal{O}$	$(3,10)$	$(10,12)$	$(12,9)$	$(10,1)$	$(3,3)$
$(10,1)$	$(10,1)$	$(3,10)$	$(12,9)$	$(12,4)$	$(10,12)$	$(7,2)$	$\mathcal{O}$	$(3,3)$	$(7,11)$
$(10,12)$	$(10,12)$	$(12,4)$	$(3,3)$	$(10,1)$	$(12,9)$	$\mathcal{O}$	$(7,11)$	$(7,2)$	$(3,10)$
$(12,4)$	$(12,4)$	$(7,11)$	$(10,12)$	$(3,10)$	$(10,1)$	$(3,3)$	$(7,2)$	$(12,9)$	$\mathcal{O}$
$(12,9)$	$(12,9)$	$(10,1)$	$(7,2)$	$(10,12)$	$(3,3)$	$(7,11)$	$(3,10)$	$\mathcal{O}$	$(12,4)$

Solution: To find Bob's message, we need to compute m, which we can do by solving $m = c_2 - a \cdot c_1$ as specified by the protocol from the slides. First, then, we need to find a by solving

$$a = \log_g(A) = \log_{(3,10)}(7, 11).$$

The easiest way to find a is by simply enumerating multiples of $(3, 10)$ using the given multiplication table until we see $(7, 11)$.

$$\begin{aligned}
\mathcal{O} \cdot (3,10) &= (3,10) \\
(3,10) \cdot (3,10) &= (10,1) \\
(3,10) \cdot (3,10) \cdot (3,10) &= (10,1) \cdot (3,10) = (12,9) \\
(3,10) \cdot (3,10) \cdot (3,10) \cdot (3,10) &= (12,9) \cdot (3,10) = (7,2) \\
(3,10) \cdot (3,10) \cdot (3,10) \cdot (3,10) \cdot (3,10) &= (7,2) \cdot (3,10) = (7,11).
\end{aligned}$$

Since $5 \cdot (3, 10) = (7, 11)$, $a = 5$. The final step is now to compute $m = c_2 - a \cdot c_1$:

$$\begin{aligned}
m &= c_2 - a \cdot c_1 \\
&= (7,2) - 5 \cdot (12,9) \\
&= (7,2) - (12,4) && \text{(using table)} \\
&= (7,2) + (12,9) && ((12,4)^{-1} = (12,9)) \\
&= (10,12). && \text{(using table)}
\end{aligned}$$

Thus $\boxed{m = (10, 12).}$

A Notation

Symbol	Translation	Example
$\in$	*"in"*	This symbol indicates *membership.* $1 \in \mathbb{Z}$, $1+i \in \mathbb{C}$, $4 \in \mathbb{Z}_5$, $a \in \{a,b,c\}$
$\notin$	*"not in"*	This symbol indicates *lack of membership.* $-2 \notin \mathbb{N}$, $1/2 \notin \mathbb{Z}$, $a \notin \{1,2,3\}$
$\forall$	*"for all"*	$C = i+1 \ \forall \ i = 1,2,\ldots,n$ $\rightarrow$ For each i from 1 to n, $C = i+1$.
$\exists$	*"there exists"*	$\forall \ x \in \mathbb{Z}$, $\exists \ y \in \mathbb{Z}$ such that $x+y=0$. $\rightarrow$ For every integer x, there exists another integer y such that $x+y=0$.
$\nexists$	*"there does not exist"*	$\nexists$ even prime p such that $p > 2$ $\rightarrow$ There does not exist an even prime number larger than 2.
$\Rightarrow$	*"implies"*	x is prime $\Rightarrow x \neq 4$ $\rightarrow$ If x is prime, then x cannot be equal to 4.
$\Leftarrow$	*"implied by"*	Exactly one of $\{x,y\}$ is odd $\Leftarrow$ the product xy is odd $\rightarrow$ If the product of two numbers x and y is an odd number, then exactly one of x and y is an odd number.
$\Leftrightarrow$	*"if and only if"*	(combination of "$\Rightarrow$" and "$\Leftarrow$") x is divisible by 2 $\Leftrightarrow$ x is even. $\rightarrow$ If x is divisible by 2, then x is even, and if x is even, then x is divisible by 2.
$\equiv_n$	*"congruent to mod n"*	$5 \equiv_4 1$, $7 \equiv_{13} 7$, $12 \equiv_5 2$
$\simeq$	*"isomorphic to"*	An isomorphism is a one-to-one structure-preserving mapping between two sets $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z} \simeq \mathbb{Z}$
φ	*mapping*	Usually indicates a mapping from one set to another (pronounced "phi")
$\rightarrow$	***general** mapping*	Indicates a general, nonspecific mapping from one set to another
$\mapsto$	***specific** mapping*	Indicates a particular mapping from elements in the domain to their images in the range
$\times$	*Cartesian product*	For two sets A and B, $A \times B$ is the set of all elements (a,b) where $a \in A$ and $b \in B$ $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$

gcd	*greatest common divisor*	Largest positive integer that divides arguments $\gcd(8,12)=4$, $\gcd(2,13)=1$
lcm	*least common multiple*	Smallest positive integer that is a multiple of arguments $\text{lcm}(3,6)=3$, $\text{lcm}(12,20)=60$
$\mathbb{Z}$	*set of all integers*	$\ldots,-2,-1,0,1,2,\ldots$
$\mathbb{Z}^+$	*set of all* ***positive*** *integers*	$1,2,3,4,5,\ldots$
$\mathbb{N}$	*set of all natural numbers*	$1,2,3,4,5,\ldots$
$\mathbb{Q}$	*set of all rational numbers*	A rational number is any number of the form m/n, where m and n are integers. $0, 1/2, -2, \ldots$
$\mathbb{Q}^+$	*set of all* ***positive*** *rational numbers*	$1/2, 10, 35/145, \ldots$
$\mathbb{R}$	*set of all real numbers*	$-6/10$, e, $10^5, \ldots$
$\mathbb{R}^+$	*set of all* ***positive*** *real numbers*	$0.11, e^2, 154, \ldots$
$\mathbb{C}$	*set of all complex numbers*	Any number of the form $a+bi$, where $a,b\in\mathbb{R}$ $1+i$, $-e+2.4i, \ldots$
$\mathbb{Z}_n$	*set of integers mod n*	$\mathbb{Z}_n=\{0,1,\ldots,n-1\}$ $\mathbb{Z}_2=\{0,1\}$, $\mathbb{Z}_5=\{0,1,2,3,4\}$
U_n	*set of units mod n*	Set of invertible elements in $\mathbb{Z}_n$ $U_{14}=\{1,3,5,9,11,13\}$

B LaTeX for beginners

LaTeX is the preferred method for typesetting any sort of math document (this document was typeset in LaTeX, e.g.). It is an extremely valuable skill to have! Typing up your homework in LaTeX is a great way to practice, and, as a bonus, it makes your work *much* easier to read (for you and for me). You don't even need to install anything locally on your computer–just use Overleaf (`https://www.overleaf.com/`) to simplify your life. It has a nice editor and syntax checker, plus a built-in dark mode.

⟶ Here is a basic guide to get you started typesetting in LaTeX: `https://www.cs.princeton.edu/courses/archive/spr10/cos433/Latex/latex-guide.pdf`
⟶ And here are some great templates for typing your homework: `https://www.overleaf.com/gallery/tagged/homework`

If you need help with anything LaTeX, just shoot me an email. I am happy to help you learn!

References

[1] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, jan 1983.

[2] Sascha Grau. Elliptic curves over finite fields. `https://www.graui.de/code/elliptic2/`.

[3] Victor J. Katz John B. Fraleigh. *A first course in abstract algebra*. Addison-Wesley, 7 edition, 2003.

[4] Robin Pollak. Pollard's $p-1$ factorization. `http://robin.pollak.io/wizard_factoring.pdf`.

[5] Lidong Zhou. Secret sharing. `https://www.cs.cornell.edu/courses/cs513/2000SP/SecretSharing.html`.