Day 2: Euclidean Algorithm and Squares for Prime Moduli

Last time, we had an in-depth discussion on the integers modulo n and how operations of addition, subtraction, and multiplication work modulo n, and briefly discussed division. Using the Euclidean Algorithm to deduce the greatest common divisor of two numbers can actually unlock the key to computing an inverse modulo n. Let's get started!

GCDs and The Euclidean Algorithm

Finding the greatest common divisor (gcd) is another concept from elementary school years that has great relevance in Number Theory, and especially in Modular Arithmetic. The presence of a gcd greater than 1 is something you should note in Question **1** of Problem Set 1. Its utility for our purposes will mainly be to help us compute inverses modulo n without having to do large amounts of multiplication (as you did in Question **1**.) For larger moduli, this becomes inefficient/cumbersome very quickly!

To begin, let's recap the notion of divisibility. You should be familiar with the notion that the integer 3 divides 12 but not 14, as 3 is a factor of 12, but not 14. We use the following formal definition:

Definition: Let $d, n \in \mathbb{Z}$. We say that d **divides** n if $n = qd$ for some $q \in \mathbb{Z}$. We write $d \mid n$ to say "d divides n".

From here, we can easily define the notion of a greatest common divisor - you may know this as the "greatest common factor".

Definition: Let $k, n \in \mathbb{Z}$ be non-zero integers. The **greatest common divisor (gcd)** of k and n is the largest *positive integer* d such that $d \mid k$ *and* $d \mid n$. We write $d = \gcd(k, n)$.

Divisibility has a lot of nice properties! Here's a few:

Theorem: Let $a, b, d \in \mathbb{Z}$. Then

(a) If $d \mid a$ then $d \mid ca$ for **any** $c \in \mathbb{Z}$.

(b) If $d \mid a$ and $d \mid b$ then $d \mid (a + b)$.

(c) $d \mid a$ and $d \mid b$ if and only if $d \mid (ax + by)$ for any $x, y \in \mathbb{Z}$.

(d) Let $k \in \mathbb{Z}$ be a common divisor of a and b; that is, $k \mid a$ and $k \mid b$. Then $k \mid \gcd(a, b)$.

The proofs of these results are left for Problem Set 2.

How do we find the gcd of two numbers? Well, you're probably used to splitting off common factors until you can't do so anymore, and collecting your result. This doesn't work well in general. For example: what is $\gcd(1955, 595)$? Or $\gcd(278783, 22103)$? The division algorithm will lend us a hand once again!

Recall from last time, our division algorithm: if $n, k \in \mathbb{Z}$, there is a unique choice of integers q and r, where $0 \leq r < k$, such that

$$n = qk + r.$$

Suppose now that $d = \gcd(n, k)$. From the theorem above, we know that as $d \mid n$ and $d \mid k$, then $d \mid (n - qk)$. Thus, $d \mid r$ as $r = n - qk$. So k and r have common factors. In fact, *they have the same* gcd *as n and k.* We can apply the division algorithm again to d and r:

$$d = q_1 r + r_1, \quad 0 \leq r_1 \leq r.$$

We can keep doing this over and over and over until we get a remainder of 0. Once we're there, we can't get any new information from the division algorithm. *Hang on... how do we know that this algorithm will end after a finite number of steps? Think about it!*

As it turns out, the last non-zero remainder from iterating the division algorithm over and over will **always** be the gcd! The process of finding the gcd from iterating the division algorithm is known as the **Euclidean algorithm**. Let's see this in action.

Example: Compute $\gcd(24, 57)$.

Solution: You should be able to tell from inspection (in this "easy" case) that the gcd is 3. We'll use the Euclidean algorithm to confirm this.

$$\begin{aligned} 57 &= 2 \cdot 24 + 9 \\ 24 &= 2 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \quad \textbf{STOP!} \end{aligned}$$

Our last non-zero remainder was 3, so $\gcd(24, 57) = 3$. ■

Note: These notes will use ■ to indicate the end of an example, and □ to indicate the end of a proof.

Example 2: Compute $\gcd(82, 32)$.

Solution: Again, we should know to expect 2 as the result here. Let's confirm.

$$\begin{aligned} 82 &= 2 \cdot 32 + 18 \\ 32 &= 1 \cdot 18 + 14 \\ 18 &= 1 \cdot 14 + 4 \\ 14 &= 3 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0 \quad \textbf{STOP!} \end{aligned}$$

Our last non-zero remainder was 2, so $\gcd(82, 32) = 2$. ■

You were promised inverses modulo n, but these are just GCDs. What gives? Well, to get inverses modulo n, we're going to have to go *backwards!* For that, we're going to need what is called the

extended Euclidean algorithm.

For integers a and b, our objective now will be to express the $\gcd(a, b)$ as a linear combination of a and b. Why we want this will become clear soon. By a linear combination of a and b, we mean an expression $ax + by$ where $x, y \in \mathbb{Z}$.

The process will be as follows: start with the final equation without zero (i.e. the one that contains the gcd as the remainder!) It should look like

$$r_{n-2} = q_{n-1}r_{n-1} + r_n, \tag{1}$$

where r_n is your gcd. Solve the equation for r_n. Now, the line above equation (1) should look like $r_{n-3} = q_{n-2}r_{n-2} + r_{n-1}$ and can be solved for r_{n-1}. Substitute this value for r_{n-1} into equation (1). You'll be tempted to expand the products involved - don't! You want to collect coefficients! Continue this process until you're at the first line of the algorithm, which involves the values a and b which you wanted the gcd of. Once you've collected the coefficients, you'll have the equation $ax + by = r_n$, where $r_n = \gcd(a, b)$.

In short: Solve every equation for the remainder in that equation. Starting with the second-last equation (i.e. when $\gcd(a, b)$ is the remainder), substitute in the expression for the remainder from the line above. Collect coefficients, then input the expression for the next remainder from above. Continue until you have $\gcd(a, b)$ as a linear combination of a and b.

All that may sound confusing without some examples. Let's apply this to our last two examples.

Example 1: Our workings from computing $\gcd(24, 57)$.

Original Equation	Solved for Remainder
$57 = 2 \cdot 24 + 9$	$9 = 57 - 2 \cdot 24$
$24 = 2 \cdot 9 + 6$	$6 = 24 - 2 \cdot 9$
$9 = 1 \cdot 6 + 3$	$3 = 9 - 1 \cdot 6$
$6 = 2 \cdot 3 + 0$	*don't rearrange this one*

Now, begin substitution. Start with $3 = 9 - 1 \cdot 6$ and substitute the expression for 6 in the equation above.

$$\begin{aligned} 3 &= 9 - 1 \cdot 6 \\ &= 9 - 1 \cdot [24 - 2 \cdot 9] \quad \textit{now, collect coefficients on } 24 \textit{ and } 9 \\ &= 3 \cdot 9 - 24 \end{aligned}$$

From here, use the expression for 9 and substitute it in.

$$\begin{aligned} 3 &= 3 \cdot 9 - 24 \\ &= 3 \cdot [57 - 2 \cdot 24] - 24 \quad \textit{now, collect coefficients on } 24 \textit{ and } 57 \\ &= 3 \cdot 57 - 7 \cdot 24. \end{aligned}$$

Therefore, $3 = 3 \cdot 57 - 7 \cdot 24$ is a linear combination of $\gcd(24, 57)$ in terms of 24 and 57. ■

Example 2: Our workings from $\gcd(82, 32)$.

Original Equation	Solved for Remainder
$82 = 2 \cdot 32 + 18$	$18 = 82 - 2 \cdot 32$
$32 = 1 \cdot 18 + 14$	$14 = 32 - 1 \cdot 18$
$18 = 1 \cdot 14 + 4$	$4 = 18 - 1 \cdot 14$
$14 = 3 \cdot 4 + 2$	$2 = 14 - 3 \cdot 4$
$4 = 2 \cdot 2 + 0$	*don't rearrange this one*

Now, start substituting upwards. We'll do this all in one shot this time.

$$\begin{aligned}
2 &= 14 - 3 \cdot 4 \\
&= 14 - 3 \cdot [18 - 1 \cdot 14] && \textit{now, collect coefficients on } 18 \textit{ and } 14 \\
&= 4 \cdot 14 - 3 \cdot 18 \\
&= 4 \cdot [32 - 1 \cdot 18] - 3 \cdot 18 && \textit{now, collect coefficients on } 32 \textit{ and } 18 \\
&= 4 \cdot 32 - 7 \cdot 18 \\
&= 4 \cdot 32 - 7 \cdot [82 - 2 \cdot 32] && \textit{now. collect coefficients on } 82 \textit{ and } 32 \\
&= 18 \cdot 32 - 7 \cdot 82
\end{aligned}$$

Therefore, $2 = 18 \cdot 32 - 7 \cdot 82$ is a linear combination of $\gcd(82, 32)$ in terms of 32 and 82. ■

So how does this help us with inverses modulo n? From Problem Set 1, we noticed that a^{-1} existed in $\mathbb{Z}_n$ when a and n had *no common factors other than* 1... a.k.a. their **greatest common divisor was 1!** So, if $\gcd(a, n) = 1$, we know from the extended Euclidean algorithm that there exists integers $x, y \in \mathbb{Z}$ such that

$$ax + ny = 1.$$

Now consider this equation modulo n. We have

$$1 \equiv ax + ny \equiv ax + 0 \equiv ax \pmod{n}.$$

Thus, as $ax \equiv 1 \pmod{n}$, we have that $a^{-1} \equiv x \pmod{n}$. Often times x will be presented as a number larger than n or negative, so you'll need to reduce it modulo n to get a^{-1}.

One last definition to round things off. For each $n \geq 2$, there are elements in $\mathbb{Z}_n$ which are invertible (gcd with n is 1), and elements which are not invertible (elements which share a common factor with n other than 1). Let's group the invertible ones together.

Definition: For $n \geq 2$, define the set $\mathbb{Z}_n^*$ to be the set of all elements in $\mathbb{Z}_n$ which have inverses; that is,

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}.$$

We call $\mathbb{Z}_n^*$ the **group of units modulo** n.

For those who attended the Group Theory sessions last year, this is an example of a group!

With that, we're ready for Problem Set 2!

Quadratic Residues: A Brief Introduction

First, recall from the Problem Set 2 that $\mathbb{Z}_p^* = \{1, 2, 3..., p-1\}$. That is, every non-zero element of $\mathbb{Z}_p$ is invertible! We'll focus our treatment to *odd* primes (i.e. $p \neq 2$ and is prime) since $\mathbb{Z}_2^* = \{1\}$ and there's nothing interesting happening there.

Definition: Let p be an odd prime and let $a \in \mathbb{Z}_p^*$. We say a is a **quadratic residue modulo** p if there exists an element $x \in \mathbb{Z}_p^*$ such that $x^2 \equiv a \pmod{p}$. That is, a is a square modulo p.

In Problem Set 1 you were asked to analyze squares modulo different values of n. Let's take a look at the squares (and non-squares) modulo primes starting at $p = 5$. For brevity, we'll truncate $x^2 \pmod 5$ as $x^2\ (5)$.

$\mathbb{Z}_5$

x	1	2	3	4
$x^2\ (5)$	1	4	4	1

squares: $1, 4$

non-squares: $2, 3$

$\mathbb{Z}_7$

x	1	2	3	4	5	6
$x^2\ (7)$	1	4	2	2	4	1

squares: $1, 2, 4$

non-squares: $3, 5, 6$

There are a few patterns at play here. For the moment, we'll focus on the fact that values of x^2 repeat in reverse order after passing $\dfrac{p-1}{2}$. Indeed, modulo 5, we have $-1 \equiv 4 \pmod 5$ and $-2 \equiv 3 \pmod 5$.

Modulo 7, we have $-1 \equiv 6 \pmod 7$, $-2 \equiv 5 \pmod 7$, and $-3 \equiv 4 \pmod 7$. In general, it makes sense that $(-x)^2 \equiv x^2 \pmod n$ as $(-x)^2 = x^2$ in the integers themselves! Thus, we can consider fewer values to build these tables. Let's do this again for $\mathbb{Z}_{11}$ and $\mathbb{Z}_{13}$.

$\mathbb{Z}_{11}$

x	±1	±2	±3	±4	±5
$x^2\ (11)$	1	4	9	5	3

squares: $1, 3, 4, 5, 9$

non-squares: $2, 6, 7, 8, 10$

$\mathbb{Z}_{13}$

x	±1	±2	±3	±4	±5	±6
$x^2\ (13)$	1	4	9	3	12	10

squares: $1, 3, 4, 9, 10, 12$

non-squares: $2, 5, 6, 7, 8, 11$

A couple of patterns are emerging from these tables. These patterns hold true for general odd primes p.

1. In $\mathbb{Z}_p^*$, **exactly** *half* of the elements are squares/residues. The other half are not.
2. Every square in $\mathbb{Z}_p^*$ has exactly 2 distinct square roots.

We'll explore these results and more in next week's session!