# Honors Discrete Mathematics: Lecture 16 Notes

*Gerandy Brito Spring 2022*

**Sarthak Mohanty**

# Congruency Classes and Applications

## Invertibility

The extended Euclidean algorithm states that given $a \geq b > 0$, where $a, b \in \mathbb{N}$, we can construct $d$ such that $d = \gcd(a, b) = a \cdot r + b \cdot s$. This leads us to Bezout's Identity:

**Bezout's Identity.** If $d = \gcd(a, b)$, then $\exists r, s \in \mathbb{Z}$ such that $d = a \cdot r + b \cdot s$.

Let's use this identity to solve the system $ax \equiv 1 \pmod{m}$. Using Bézout's Theorem, we need that $\gcd a, m = 1$.

$$\begin{aligned} 1 &= a \cdot s + m \cdot t \\ 1 &= a \cdot s \pmod{m}, \end{aligned}$$

so $s$ is a solution.

**Definition.** Given $\bar{a} \in \mathbb{Z}$, the *inverse* of $\bar{a}$ is $\bar{b}$ such that $\bar{a}\bar{b} = \bar{1}$.
**Claim.** The inverse is unique

## Chinese Remainder Theorem

As discussed last class, recall the Chinese Remainder Theorem, or CRT:

**Definition.** Let $m_1, m_2, \ldots, m_k \in \mathbb{N}^*$ such that $\gcd(m_i, m_j) = 1$ for all $1 \leq i < j \leq k$. Also let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. The system

$$\begin{cases} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{cases}$$

has a unique solution $\mod M = m_1 m_2 \ldots m_k$.

*Proof of Existence.* Let

$$M_i = \frac{M}{m_i} = m_1 \cdot m_2 \cdot m_3 \cdot \cdots \cdot m_{i-1} \cdot m_{i+1} \cdot m_k.$$

such that $\gcd(m_i, M_i) = 1$. Then we have

$$x = \cancelto{0}{a_1 y_1 M_1} + \cdots + \cancelto{0}{a_{i-1} y_{i-1} M_{i-1}} + a_i y_i M_i + \cancelto{0}{a_{i+1} y_{i+1} M_{i+1}} + \cdots + \cancelto{0}{a_k y_k M_k} \equiv \cancelto{1}{y_i M_i} a_i \equiv a_i \pmod{m_i}$$

where $y_i \cdot M_i \equiv 1 \pmod{m_i}$; in other words, $y_i$ is the inverse of $M_i$ mod $m_i$.

*Proof of "Uniqueness".* Let $x, \hat{x}$ be two solutions. Then

$$x_1 \equiv x_2 \equiv a_i \quad (\forall i)(1 \leq i \leq k).$$

Then by definition $x_1 - x_2$ is a multiple of $m_i$. But then $M = m_1 m_2 \ldots m_k$ divides $x_1 - x_2$. By definition, this means $x_1 \equiv x_2 \pmod{M}$. If $x_1, x_2 < M$, this means $x_1 = x_2$.

## Examples

1. P1 (IMO 1959) Show that $\frac{21n+4}{14n+3}$ is irreducible for all $n \in \mathbb{N}$.

*Proof.* Recall $\gcd(a, b) = \gcd(b, a - b)$. Hence

$$\begin{aligned} \gcd(21n + 4, 14n + 3) &= \gcd(14n + 3, 7n + 1) \\ &= \gcd(7n + 1, 7n + 2) \\ &= \gcd(7n + 1, 1) = 1 \end{aligned}$$

2. Consider the sequence $\{a_n\}_{n\in\mathbb{N}}$, where $a_n = 100 + n^2$. Let $d_n = \gcd(a_n, a_{n+1}$. find the largest value of $d$.

Solution. In other words, we are looking for

$$\gcd(100 + n^2, 100 + n^2 + 2n + 1) = \gcd(100 + n^2, 2n + 1)$$

Note that $2n + 1$ is always odd. We claim that $d$ is always odd, since the divisor of an odd number must be odd. We now make the following claim:

If $d = \gcd(a, b)$ is odd and $b$ is odd, then $d = \gcd(2^k a, b)$, where
We can now simplify

$$\begin{aligned}
\gcd(100 + n^2, 2n + 1) &= \gcd(400 + 4n^2, 2n + 1) \\
&= \gcd((2n + 1)^2 - 4n - 1 + 400, 2n + 1) \\
&= \gcd((2n + 1)^2 - 4n + 399, 2n + 1) \\
&= \gcd(-4n + 399, 2n + 1) \\
&= \gcd(-4n + 399, 4n + 2) \\
&= \gcd(401, 4n + 2)
\end{aligned}$$

Check for $n = 200$.

# Post-Lecture

## Question 1

Show that $4^{1536} - 9^{4824}$ is a multiple of 35.

## Solution

By definition, it suffices to check that $9^{4824} \equiv 4^{1536} \pmod{35}$. Using the Chinese Remainder Theorem, both of the following equivalencies hold:

$$\begin{aligned}
9^{4824} &\equiv 4^{1536} \pmod{5} \\
9^{4824} &\equiv 4^{1536} \pmod{7}.
\end{aligned}$$

We now use the rule that if $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

$$\begin{aligned}
9^{4824} &\equiv (-1)^{4824} = 1 \pmod{5} \\
4^{1536} &\equiv (-1)^{1536} = 1 \pmod{5}.
\end{aligned}$$

Thus $9^{4824} \equiv 4^{1536} \equiv 1 \pmod{5}$.
Now

$$\begin{aligned}
9^{4824} &\equiv 2^{4824} \pmod{7} = 2^{3\cdot 1608} = (8)^{1608} \equiv 1^{1608} = 1 \pmod{7} \\
4^{1536} &= 4^{3\cdot 512} = 64^{512} \equiv 1^{512} \equiv \pmod{7}.
\end{aligned}$$

Thus $9^{4824} \equiv 4^{1536} \equiv 1 \pmod{7}$, and by CRT we have our desired result.