Honors Discrete Mathematics: Lecture 14 Notes

Gerandy Brito Spring 2022

Sarthak Mohanty

Operations on Congruency Classes

Example. Find all integer solutions to the equation

$$6x + 2y^2 = 2020$$

Solution. We will work step by step.

1. For any $m \in \mathbb{Z}$, we have $6x + 2y^2 \equiv 2020 \pmod{m}$. We will use $m = 3$. We will first show that $y^2 \equiv 0$ or $1 \pmod{3}$ for any $y \in \mathbb{Z}$.

   For any $y \in \mathbb{Z}$, either $3 \mid y$ or $3 \nmid y$.

   Case 1. Suppose $3 \mid y$. Then $y \equiv 0 \pmod{3}$, so $y^2 \equiv 0 \pmod{3}$.

   Case 2. Suppose $3 \nmid y$. Then $y \equiv 1$ or $2 \pmod{3}$.

   Case 2.1. Suppose $y \equiv 1 \pmod{3}$. Then $y^2 \equiv 1^2 \equiv 1 \pmod{3}$.

   Case 2.2. Suppose $y \equiv 2 \pmod{3}$. Then $y^2 \equiv 2^2 \equiv 1 \pmod{3}$.

   In either subcase, $y^2 \equiv 1 \pmod{3}$.

   In either case, $y^2 \equiv 0$ or $1 \pmod{3}$.

2. Now we can show that $6x + 2y^2 \equiv 0$ or $2 \pmod{3}$ for all pairs $x, y \in \mathbb{Z}$.

   For any $y \in \mathbb{Z}$, either $y^2 \equiv 0 \pmod{3}$ or $y^2 \equiv 1 \pmod{3}$.

   Case 1. Suppose $y^2 \equiv 0 \pmod{3}$. Then $6x + 2y^2 \equiv 6x \equiv 0 \pmod{3}$ for all $x \in \mathbb{Z}$.

   Case 2. Suppose $y^2 \equiv 1 \pmod{3}$. Then $6x + 2y^2 \equiv 6x + 2 \equiv 2 \pmod{3}$ for all $x \in \mathbb{Z}$.

   In either case, $6x + 2y^2 \equiv 0$ or $2 \pmod{3}$ for all $x \in \mathbb{Z}$.

3. Finally, let $x, y \in \mathbb{Z}$. Now note that $2020 \equiv 1 \pmod{3}$. But from part (b), $6x + 2y^2 \not\equiv 1 \pmod{3}$, so $6x + 2y^2 \not\equiv 2020 \pmod{3}$, so $6x + 2y^2 \neq 2020$. Therefore there exist no integer solutions to the equation $6x + 2y^2 = 2020$.

Divisibility Rules

Theorem. A number n is divisible by 3 iff the sum of its digits (in base 10) is also a multiple of 3.

Proof. Let $n = n_k n_{k-1} n_{k-2} \ldots n_1 n_0$, where $n_i \in \{0, 1, \ldots, 9\}$. Note that

$$\begin{aligned} 10 &\equiv 1 \pmod{3} \\ 10^2 &\equiv 1 \pmod{3} \\ &\vdots \\ 10^t &\equiv 1 \pmod{3} \end{aligned} \tag{$*$}$$

Then

$$\begin{aligned} n &= \cancelto{1}{10^k} \cdot n_k + \cancelto{1}{10^{k-1}} \cdot n_{k-1} + \cdots + \cancelto{1}{10} \cdot n_1 + n_0. \\ &\overset{(*)}{\equiv} n_k + n_{k-1} + \cdots + n_1 + n_0 \pmod{3}. \end{aligned}$$

Tricks

Let's find $10^{2022} \pmod{7}$.

First note that $\{10^k\}_{k\geq 1} \pmod 7$ is periodic, as we will show below.

$$\begin{aligned}
&10^1 \equiv 3 \pmod 7\\
&10^2 \equiv 2 \pmod 7\\
&10^3 \equiv 10^2 \cdot 10 \equiv 2 \cdot 3 = 6 \pmod 7\\
&10^4 \equiv 10^3 \cdot 10 \equiv 6 \cdot 3 \equiv 4 \pmod 7\\
&10^5 \equiv 10^4 \cdot 10 \equiv 4 \cdot 3 \equiv 5 \pmod 7\\
&10^6 \equiv 10^5 \cdot 10 \equiv 5 \cdot 3 \equiv 1 \pmod 7\\
&10^7 \equiv 10^6 \cdot 10 \equiv 1 \cdot 3 = 3 \pmod 7
\end{aligned}$$

The sequence $3, 2, 6, 4, 5, 1$ will repeat as we take larger powers of 10.

Now $10^{2022} = 10^{6\cdot q+r} \equiv 1 \pmod 6$,, since the sequence repeats every 6 values.

Fermat's Little Theorem

To introduce this theorem, we first state a lemma.

Lemma Take some prime number p and some integer a. Then $\{i \cdot a\}_{1\leq i\leq p-1}$ are all diff $\pmod p$
Proof (By contradiction) Assume there are $1 \leq i, j \leq p-1$ such that $ia \equiv ja \pmod p$ OR $(i-j)a \equiv 0 \pmod p$ contradiction! (unless $i = j$).
Using this lemma, Fermat observed that $(*)$

$$\begin{aligned}
a^{p-1}(p-1)! &\equiv (p-1)! \pmod p\\
(a^{p-1}-1)(p-1)! &\equiv 0 \pmod p
\end{aligned}$$

Finally, he created his own theorem, stated below.

Fermat's Little Theorem. For any prime number p and integer a, $a^{p-1} \equiv 1 \pmod p$.

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k \in \mathbb{N}^*$ such that every distinct pair m_i, m_j is pairwise coprime. Also consider any $a_1, a_2, \ldots, a_k \in \mathbb{Z}$.
There exists exactly one x (taken mod m) such that

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

Proof. We construct a solution

$$M_i = \frac{M}{m_i}.$$

First set $y_i \in \mathbb{Z}$ such that $y_i \cdot M_i \equiv 1 \pmod{m_i}$. Then set

$$x = a_1y_1M_1 + a_2y_2M_2 + \cdots + a_{i-1}y_{i-1}M_{i-1} + a_iy_iM_i + a_{i+1}y_{i+1}M_{i+1} + \cdots + a_ky_kM_k.$$

Claim: $x \equiv a_i \pmod{m_i}$, because every term goes to zero except $a_iy_iM_i$, which goes to a_i.