# Math 74, Week 6

Tianshuang (Ethan) Qiu

October 9, 2021

## 1 Mon Lec, 4c

Non of the number repeating means that it is a rearrangement of the set of remainders $\{1, 2, ...6\}$. We first show that if $a \not\equiv b \mod 7, \text{then} 4a \not\equiv 4b \mod 7$
Proof: Suppose for contradiction that $4a \equiv 4b \mod 7$, then we have $7 \mid 4(a-b)$. Since $\gcd(4, 7) = 1$, $7 \mid a - b$, $a \equiv b \mod 7$, $\lightning$. We have a contradiction, therefore $4a \not\equiv 4b \mod 7$
Let $a = 1, b = 2, 3, 4, 5, 6$. We can see that $(4 \times 1)...(4 \times 6) \equiv 6! \mod 7$. Since $6!$ is coprime with 7, we can divide it, leaving us with

$$4^6 \equiv 1 \mod 7$$

## 2 Mon Lec, 5a

Using the formula

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

$$\phi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5}) = 4$$

## 3 Mon Lec, 6

We simplify

$$\frac{x + 2k}{3} \leq x + 1$$

$$x + 2k \leq 3x + 3$$

$$2x \geq 2k - 3$$
$$x \geq \frac{2k-3}{2}$$

So $(2k-3)/2 = 3, 2k = 9, k = 4.5$

## 4 Mon Dis, 2b

$$17^{1707} \bmod 11 \equiv 6^{1707} \bmod 11$$

By fermats little theorem $6^{1}0 \equiv 1 \bmod 11$

$$6^{1}707 \equiv (6^{1}0)^{1}70 \times 6^{7} \bmod 11 \equiv 6^{7} \bmod 11$$

Now we start raising 6 to higher powers.

$$6^2 \equiv 3 \bmod 11$$

$$6^4 \equiv 9 \bmod 11$$

$$6^7 \equiv 3 \times 9 \times 6 \bmod 11 \equiv 8 \bmod 11$$

So $17^{1707} \equiv 8 \bmod 11$

## 5 Mon Dis, 4c

We first compute $\phi(100)$

$$\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$$

Since $\gcd(43, 100) = 1$, we can apply Euler Totient theorem.

$$43^{1763} \equiv (43^{40})44 \times 43^3 \equiv 43^3 \bmod 100$$

$43^2 = 1849 \equiv 49 \bmod 100$, so $43^3 \equiv 49 \times 43 \bmod 100$ Finally we get $43^3 \equiv 7 \bmod 100$

# 6 Wed Lec, 2a

We factor the expression into $n(n^2 - 1) = n(n+1)(n-1)$
Integers that are divisible by 2 are spaced such that there is one every other, and those divisible by 3 are spaced such that there is one every third. Here we have a product of 3 consecutive integers, so there must be at least 1 integer between $n-1, n, n+1$ that is divisible by 2, and at least 1 that is divisible by 3. Since $6 = 2 \times 3$, we have $6 \mid n(n+1)(n+2)$.
Thus we have proven that $6 \mid n^3 - n$
$\blacksquare$

# 7 $2021^{4042}$ mod 100

First we since 2021 is odd and does not end in 5 or 0, $\gcd(2021, 100) = 1$, so we can apply the Euler Totient Theorem.

$$\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$$

$$2021^{4042} \equiv (2021^{40})101 \times 2021^2 \equiv 2021^2 \equiv 21^2 \bmod 100$$

Now we can simply calculate the square to be $441 \equiv 41 \bmod 100$

# 8 Wed Dis 1a

First we show that $17n^2 + 1 \not\equiv 0 \bmod 4$
$17n^2 + 1 \equiv n^2 + 1 \bmod 4$ Now we assume that there exists some $n \geq 1$ that sataisfies this equation. Then we have $n^2 + 1 \equiv 0 \bmod 4$

$$n^2 \equiv 3 \bmod 4$$

Now we consider all the possibilities of $n \mod 4$: $1^2 \equiv 1, 2^2 \equiv 0, 3^3 \equiv 1, 4^2 \equiv 0 (\mathrm{mod} 5)$. Therefore there is no way $n$ that sataisfies $n^2 \equiv 3$. Our assumption is incorrect and $4 \not| 17n^2 + 1$
We repeat the proof for mod5
$17n^2 + 1 \equiv 2n^2 + 1 \bmod 5$ We assume that there exists some $n \geq 1$ that sataisfies this equation. Then we have $2n^2 + 1 \equiv 0 \bmod 5$

$$2n^2 \equiv 4 \bmod 5$$

$$n^2 \equiv 2 \bmod 5$$

We can examine the possible squares: $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1 (\mathrm{mod} 5)$
Once again there is no possible way for $n^2$ to be 2. Our assumption is incorrect and $5 \not| 17n^2 + 1$
Thus we have proven both parts of the hypothesis. ■

# 9 Wed Dis, 5