Exponents in modular arithmetic

Dennis Chen, Kelin Zhu

NQT

1 Fermat's Little Theorem

Often in number theory problems we will want to take some number to some large power and find its remainder when divided by another number. Fermat's Little Theorem provides a way to make this calculation much easier.

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

If we add the restriction that a and p are relatively prime, we can divide by a on both sides to achieve the following.

Fermat's Little Theorem, alternative. Consider a prime p. For relatively prime a, p, $a^{p-1} \equiv 1 \pmod{p}$.

There are two proofs for this theorem. We present the induction proof first because it requires the least amount of ingenuity.

Proof 1 (Induction). For the inductive proof, we prove that $a^p \equiv a \pmod{p}$.
This is obviously true for the base case $a = 1$.
Now assume that this is true for $a = n$. Then

$$(n+1)^p \equiv n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + 1 \pmod{p}.$$

But notice that $\binom{p}{1}, \binom{p}{2} \ldots \binom{p}{p-1}$ are all divisible by p, so

$$n^p + \binom{p}{1}n^{p-1} + \binom{p}{2}n^{p-2} + \cdots + 1 \equiv n^p + 1 \equiv n + 1 \pmod{p},$$

as desired.

The rearrangement proof requires a little bit more creativity and is more aesthetic. It can also be generalized to Euler's Theorem, where the first proof cannot.

Proof 2 (Rearrangement). Suppose that a and p are relatively prime. We claim that $a, 2a, 3a \ldots a(p-1)$ is a rearrangement of $1, 2, 3 \ldots p-1$ taken mod p. We prove this by contradiction. Assume that there are two integers such that $ax \equiv ay \pmod{p}$ with $0 < x, y < p$ and $x \neq y$. Since $\gcd(a, p) = 1$, we can divide both sides by a to yield $x \equiv y$. But this is obviously not possible. Thus, contradiction.
This implies that $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$. As $\gcd(p, (p-1)!) = 1$, we can divide both sides by $(p-1)!$ to get $1 \equiv a^{p-1} \pmod{p}$, as desired.

Here are some basic examples of Fermat's Little Theorem.

Example. Find the remainder of $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ when divided by 7.

Solution. Note that

$$\begin{aligned} 2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} &\equiv 2^2 + 3^0 + 4^4 + 5^2 + 6^0 \\ &\equiv 4 + 1 + 256 + 25 + 1 \\ &\equiv 0 \pmod 7. \end{aligned}$$

Example (AMC 12A 2008/15). Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

Solution. This is a mixture of Chinese Remainder Theorem and Fermat's Little Theorem.
Obviously $2 \mid k^2 + 2^k$, so we can consider its remainder when divided by 5. Now note that

$$k \equiv 2008^2 + 2^{2008} \equiv 3^2 + 2^0 \equiv 0 \pmod 5.$$

Since $5 \mid k$ and $4 \mid k$,

$$k^2 + 2^k \equiv 2^k \equiv 1 \pmod 5.$$

Now by CRT Congruences,

$$\begin{aligned} 0 &\equiv 6 \pmod 2 \\ 1 &\equiv 6 \pmod 5, \end{aligned}$$

so the remainder when divided by 10 is 6 as well.

Here's a pedagogical example of Fermat's and Chinese Remainder Theorem.

Example (42 PMO Level 3 2020/1). Let $p_1, p_2, \ldots, p_n$ be distinct prime numbers and P be their product. Let the number S be defined as

$$S = \sum_{i=1}^{n} \left(\frac{P}{p_i}\right)^{p_i - 1}.$$

Show that $S - 1$ is a multiple of P.

Solution. Note that $S \equiv \left(\frac{P}{p_k}\right)^{p_k - 1} \equiv 1 \pmod{p_k}$ by Fermat's Little Theorem, so $S \equiv 1 \pmod P$ by CRT.

1.1 Monic Monomials mod n

The important idea is that monic monomials **don't always cover all residues** mod n for certain n.
We begin with perhaps the most famous and often used example.

Example (Quadratic Residues mod 4). The only positive integers $0 \le k < 4$ such that $n^2 \equiv k \pmod 4$ has a solution are $k = 0$ and $k = 1$.

In other words, the remainder of a square divided by 4 is always 0 or 1.

Solution. Just plug in $0, 1, 2, 3$ and check only $0, 1$ are outputted.

Example (Macedonia JBMO TST 2016/1). Solve

$$x_1^4 + x_2^4 + ... + x_{14}^4 = 2016^3 - 1$$

over the integers.

Solution. There are no solutions. Take mod 16 and note that $x^4 \in \{0, 1\} \pmod{16}$ and $2016^3 - 1 \equiv 15 \pmod{16}$.

With practice and experience, these patterns will become clearer over time. For instance, fourth powers strongly suggest taking mod 16, and squares strongly suggest taking mod 4, mod 3, or mod 8, depending on the context.

Speaking of squares and mod 3 . . .

Example (USAJMO 2011/1). Find, with proof, all positive integers n for which $2^n + 12^n + 2011^n$ is a perfect square.

Solution. We claim the only solution is $n = 1$, since $2 + 12 + 2011 = 2025 = 45^2$.

Now we claim that no solutions $n > 1$ work. Assume otherwise. Then note that for mod 3 reasons, we must have n be odd since $2^n + 2011^n \equiv 2^n + 1^n \equiv 2^n + 1 \pmod{3}$, and we must have it be congruent to 0 mod 3. But also note for mod 4 reasons, we must have n be even since $2011^n \equiv (-1)^n \pmod{4}$, and we must have it be congruent to 1 mod 4, contradiction.

1.2 Exponential Functions mod n

You will also want to consider exponential functions mod n. The idea is you can use Fermat's Little Theorem to figure out the residues the function is restricted to.

We start with an easier problem as an example.

Example (April USAJMO 2020/1). Determine, with proof, whether there exists a positive integer n such that $4^n - 1$ divides $5^n - 1$.

Solution. Clearly $3 \mid 4^n - 1$ so we must have $3 \mid 5^n - 1$, implying that $2 \mid n$. But also note that $2 \mid n$ implies $5 \mid 4^n - 1$, contradiction.

Exponential functions usually go hand in hand with bounding and size arguments.

Example (TurtleKing123). Find all ordered triplets of natural numbers (a, b, c) such that

$$6^a + 7^b = 13^c.$$

The proof of the $a = 1$ case is better suited for the Prime Factorization unit, but the rest is quite informative for this unit.

Solution. We claim the answer is just $a = b = c = 1$, and it is easy to check that it works.

Assume $a > 2$. The cases $a = 1$ and $a = 2$ will be shown later.

Taking mod 4 gives us that b is even, and then taking mod 8 gives c is even as well. Let $2x = b$ and $2y = c$. Then

$$(13^x - 7^y)(13^x + 7^y) = 6^a.$$

Note that for mod 3 reasons all powers of 3 are concentrated in $13^x - 7^y$, so $13^x + 7^y$ must be of the form 2^k. But this implies that $3^k \mid 13^x - 7^y$, absurd for size reasons.

For $a = 2$ note that taking mod 14 gives that b is even and c is odd, but mod 14 gives that b is odd and c is even, contradiction.

For $a = 1$, subtract 13 to get

$$7^b - 7 = 13^c - 13.$$

The first main claim is that $43 \mid 7^b - 7$. Note that $12 \mid b - 1$ since the smallest number k such that $7^k \equiv 1 \pmod{13}$ is 12, so $43 \mid 7^{12} - 1 \mid 7^b - 7$.

The second main step is proving $14 \mid c - 1$. Note that $7 \mid k$ where k is the smallest number such that $13^k \equiv 1 \pmod{43}$, since $13^6 \equiv 6 \pmod{43}$, implying $7 \mid c - 1$. Also for mod 7 reasons, $2 \mid c - 1$, which implies that $14 \mid c - 1$. Then note that by LTE, $49 \mid 13^{14} - 1$, so $49 \mid 13^c - 13$. Thus $49 \mid 7^b - 7$, which is only possible if $b = 1$.

Now we present a much harder example. If you don't know what the order of a number modulo a prime is, the idea is that $\text{ord}_p\, n$ is the smallest integer k such that $n^k \equiv 1 \pmod{p}$.[1]

Example (SJMO 2020/1). Find all positive integers $k \geq 2$ for which there exists some positive integer n such that the last k digits of the decimal representation of $10^{10^n} - 9^{9^n}$ are the same.

Solution. We claim only $2 \leq k \leq 4$ works. It suffices to just provide a construction for $k = 4$, and said construction is $n = 25$. We verify this works later in the proof.

We show that the only way to have the last two digits be the same is for them to both be 11. Note

$$10^{10^n} - 9^{9^n} \equiv -9^{9^n} \equiv -1 \pmod{4}$$

$$10^{10^n} - 9^{9^n} \equiv -9^{9^n} \pmod{25}.$$

Now note that $9^{10} \equiv 1 \pmod{25}$ by Euler's Theorem, so $9^{9^n} \equiv 9^{(-1)^n} \equiv 9, 14 \pmod{25}$. Thus the only possible remainders of -9^{9^n} divided by 100 are $-9, -89$, or $91, 11$. So 11 is the only possible ending 2 digits.

Now this implies we want to solve $10^{10^n} - 9^{9^n} \equiv -9^{9^n} \equiv 10^0 + 10^1 + \cdots + 10^{k-1} \pmod{10^k}$. This is valid because if $10^{10^n} \leq 10^{k-1}$ this is obviously not true. In other words,

$$9^{9^n} \equiv 8(10^0 + 10^1 + \cdots + 10^{k-1}) + 1 \equiv \frac{8(10^k - 1)}{9} + 1 \equiv \frac{1}{9} \pmod{10^k},$$

or $9^{9^n+1} \equiv 1 \pmod{10^k}$.

Now we show that $n = 25$ works for $k \geq 4$. Note that the smallest number k such that $3^k \equiv 1 \pmod{2^4}$ is $k = 4$, and $4 \mid 2(9^{25} + 1)$ and $\phi(5^4) = 4 \cdot 5^3$, and $4 \cdot 5^3 \mid 2(9^{25} + 1)$, where $4 \mid 2(9^{25} + 1$ is obvious and $5^3 \mid 9^{25} + 1$ follows from LTE as $v_5(9^{25} + 1) = v_5(9 + 1) + v_5(25) = 3$.

Now we prove $k > 4$ doesn't work. Note that the minimal k such that $3^k \equiv 1 \pmod{2^5}$ is $k = 8$, and $8 \nmid 2(9^n + 1)$ as $9^n + 1 \equiv 2 \pmod{4}$. Thus there are no solutions to $9^{9^n+1} \equiv 1 \pmod{2^k}$ for $k > 4$.

2 Euler's Totient Function

Now we take a look at Euler's Totient Function.

Euler's Totient Function. We define $\phi(n)$ to be the number of positive integers less than or equal to n that are also relatively prime to n.

[1] I also recommend you skip this example for now if you don't know what order is.

Multiplicativity. For relatively prime m, n, $\phi(m) \cdot \phi(n) = \phi(mn)$.

The basic idea of the proof is just using CRT to find all possible congruences.

Proof. Note that we can have

$$x \equiv j_1, j_2, \ldots, j_{\phi(m)} \pmod{m}$$
$$x \equiv k_1, k_2, \ldots, k_{\phi(n)} \pmod{n},$$

where j_i encompasses the numbers between 1 and m relatively prime to m and k_i encompasses the number between 1 and n relatively prime to n. Then note that this system has $\phi(m)\phi(n)$ solutions when taken mod mn.

Product Formula. Say the prime factorization of positive integer n is $p_1^{e_1} \cdot p_2^{e_2} \ldots p_k^{e_k}$. Then $\phi(n) = n\frac{p_1-1}{p_1} \cdot \frac{p_2-1}{p_2} \cdots \frac{p_k-1}{p_k}$.

Proof. Instead of actually proving this fully, we outline it for the reader to work through themselves.

1. Find $\phi(p_1^{e_1})$.
2. Use multiplicity to find $\phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$.

Euler's Totient Theorem. For relatively prime a, n, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. This is very similar to the rearrangement proof for Fermat's Little Theorem.[2]

Let the set of positive integers less than and relatively prime to n be $x_1, x_2, \ldots, x_{\phi(n)}$. Then note that $ax_1, ax_2, \ldots, ax_{\phi(n)}$ is a rearrangement of $x_1, x_2, \ldots, x_{\phi(n)}$.

We proceed by contradiction. Assume that there are two integers such that $ax \equiv ay \pmod{n}$. Since $\gcd(a, n) = 1$, we can divide both sides by a to yield $x \equiv y$. But this is obviously not possible. Thus, contradiction.

This implies that $x_1x_2 \ldots x_{\phi(n)} \equiv (x_1x_2 \ldots x_{\phi(n)})a^{\phi(n)} \pmod{n}$. Dividing both sides by $x_1x_2 \ldots x_{\phi(n)}$ yields $a^{\phi(n)} \equiv 1 \pmod{n}$, as desired.

Also, notice that Fermat's is just a special case of Euler's.

3 Problems

Minimum is [43 ♟]. Problems denoted with ♞ are required. (They still count towards the point total.)

> "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain."
>
> Pierre de Fermat

[2] So similar, in fact, that I copy-pasted the proof for Fermat's and made minor adjustments.

[1 ♟] **Problem 1 (Mathcounts National Countdown 2018)** What is the remainder when 2018^{2018} is divided by 20?

[1 ♟] **Problem 2 (PUMaC Div. A NT 2020/1)** Compute the last two digits of
$9^{2020} + 9^{2020^2} + \ldots + 9^{2020^{2020}}$.

[2 ♟] **Problem 3 (AMC 10B 2018/16)** Let $a_1, a_2, \ldots, a_{2018}$ be a strictly increasing sequence of positive integers such that

$$a_1 + a_2 + \cdots + a_{2018} = 2018^{2018}.$$

What is the remainder when $a_1^3 + a_2^3 + \cdots + a_{2018}^3$ is divided by 6?

[2 ♟] **Problem 4** Prove $\phi(n)$ is composite for $n \geq 7$.

[3 ♟] **Problem 5 (PUMaC 2018)** Find the number of positive integers $n < 2018$ such that $25^n + 9^n$ is divisible by 13.

[4 ♟] **Problem 6** Find the remainder of $5^{31} + 5^{17} + 1$ when divided by 31.

[4 ♞] **Problem 7 (MAST Diagnostic 2021)** Find the remainder of $(1^3)(1^3+2^3)(1^3+2^3+3^3)\ldots(1^3+2^3+3^3\cdots+99^3)$ when divided by 101.

[6 ♟] **Problem 8 (USAMO 1979/1)** Determine all non-negative integral solutions $(n_1, n_2, \ldots, n_k)$, if any, apart from permutations, of the Diophantine equation

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

[9 ♟] **Problem 9 (IMO 2005/4)** Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1, \ n \geq 1.$$

[9 ♟] **Problem 10 (AIME II 2020/13)** Find the least positive integer n for which $2^n + 5^n - n$ is a multiple of 1000.

[13 ♟] **Problem 11 (USEMO 2019/4)** Prove that for any prime p, there exists a positive integer n such that

$$1^n + 2^{n-1} + 3^{n-2} + \cdots + n^1 \equiv 2020 \pmod{p}.$$

3.1 Period of a Repeating Decimal

[2 ♟] **Problem 12** We define the cycle of a repeating fraction $\frac{m}{n}$ as the minimum number i such that $\frac{m}{n} = 0.\overline{a_1 a_2 a_3 \ldots a_i}$. Find the cycle of $\frac{1}{13}$ and $\frac{1}{23}$.

[3 ♟] **Problem 13 (AMC 10A 2019/18)** For some positive integer k, the repeating base-k representation of the (base-ten) fraction $\frac{7}{51}$ is $0.\overline{23}_k = 0.232323\ldots_k$. What is k?

[4 ♞] **Problem 14 (e-dchen Mock MATHCOUNTS)** What is the sum of all odd n such that $\frac{1}{n}$ expressed in base 8 is a repeating decimal with period 4?

[6 ♟] **Problem 15 (AMC 12A 2014/23)** The fraction

$$\frac{1}{99^2} = 0.\overline{b_{n-1} b_{n-2} \ldots b_2 b_1 b_0},$$

where n is the length of the period of the repeating decimal expansion. What is the sum $b_0 + b_1 + \cdots + b_{n-1}$?