Order and Maps from Finite Fields to $\mathbb{Z}_p$

Andy Jung and Gregory Pylypovych
BCA Math Team Advanced Number Theory Handout
September 28, 2019

A lot of advanced number theory problems are based on manipulation of mod equations. Two ways to do this are through order and maps.

§1 Order

In mod questions, we often want to find some k such that $a^k \equiv 1 \pmod{b}$. We define the $ord_b(a)$ or the order of a (mod b) as the smallest positive integer d such that $a^d \equiv 1 \pmod{b}$. For example, $ord_3(2) = 2$ and $ord_7(3) = 6$.
The most important property of the order is that : $ord_b(a) \mid e \iff a^e \equiv 1 \pmod{b}$.
Combining this with Euler's Totient Theorem which states $(a, b) = 1 \rightarrow a^{\phi(b)} \equiv 1 \pmod{b}$ where $\phi(b)$ is the number of relatively prime positive integers less than b, gives us that $ord_b(a) \mid \phi(b)$. Substituting b as some prime p gives us that $ord_p(a) \mid (p-1)$.
In general, we want to use order in problems involving powers and 1.

Example 1.1

(2019 AIME I 14)
Find the least odd prime factor of $2019^8 + 1$

Let our answer be a prime p. $p \mid 2019^8 + 1 \rightarrow 2019^8 \equiv -1 \pmod{p}$. $\rightarrow 2019^16 \equiv 1 \pmod{p}$. $\rightarrow ord_p(2019) \mid 16$. $2019^8 \equiv -1 \pmod{p}$. $ord_p(2019) \mid 16$. If $ord_p(2019)$ is 1, 2, 4, or 8, $2019^8 \equiv 1 \pmod{p}$, but $2019^8 \equiv -1$, so $ord_p(2019) = 16$. Because $2019^{\phi(p)} \equiv 1$ mod p, $16 \mid \phi(p) = p - 1$. The two smallest primes that satisfy this is p=17 and 97, of which 97 works.

§2 Maps from Finite Fields to $\mathbb{Z}_p$

If you look back at the statement we had for Fermat's Little Theorem, we can notice that we used the concept of a **map** in the proof. The map $f(x) : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ that maps $x \longrightarrow a \cdot x$ for some constant a. Noticing that that this map is bijective from $\mathbb{Z}_p$ to $\mathbb{Z}_p$, this means that the set of x we plug into $f(x)$ is the same as the set of the $f(x)$ that are outputed. This gives us many useful properties that we can use about these two sets, such as the products of their non-zero elements being equal modulo p. So we get that $(p-1)! \equiv (p-1)! \cdot a^{p-1}$mod p, which means that $a^{p-1} \equiv 1$mod p. But the surprising thing is that in proving Euler's theorem, this approach takes very little effort to generalize, simply noting that the map $g(x) : \mathbb{U}_m \longrightarrow \mathbb{U}_m$ that maps $x \longrightarrow a \cdot x$ for some constant a that is relatively prime to m, and following the same steps. This idea of analyzing maps is key in many number theory problems on AIME/HMMT/PUMAC, and has applications on olympiads too.

Example 2.1 Find the remainder when

$$\prod_{n=2}^{99}(1-n^2+n^4)(1-2n^2+n^4)$$

is divided by 101.(PUMAC 2018 NT 6).

Solution: $\prod_{n=2}^{99}(1-2n^2+n^4)=\prod_{n=2}^{99}(n-1)^2(n+1)^2=(\frac{100!}{1\cdot 2})^2(\frac{100!}{-1\cdot -2})^2=\frac{1}{16}$. As for the other product, $\prod_{n=2}^{99}(1-n^2+n^4)=(2-100)(2-100)\prod_{n=2,n\neq\pm 10}^{99}\frac{n^6+1}{n^2+1}=9\cdot 1=9$, as if one considers the map $f(x):\mathbb{Z}_p\longrightarrow\mathbb{Z}_p$ that maps $x^2\longrightarrow x^6$, this map is just a map from $x\longrightarrow x^3$, and since 100 is not divisible by 3, this map is bijective (proof for this is an exercise in the problem set).Hence the answer is just $\frac{9}{16}\equiv\boxed{70}$mod 101.

Another very important and commonly appearing map is the $f(x):\mathbb{Z}_p\longrightarrow\mathbb{Z}_p$ that maps $x\longrightarrow x^2$. Note that for all odd primes $2|p-1$, so since $a^{p-1}\equiv 1(\text{mod p})$, $(a^2)^{\frac{p-1}{2}}\equiv 1(\text{mod p})$, but $x^{\frac{p-1}{2}}-1$ has at most $\frac{p-1}{2}$ roots, so a^2 can take at most $\frac{p-1}{2}$ values for invertible a. But everything is a root of a^p-a, so everything is a root of $a(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)$, but $(a^{\frac{p-1}{2}}+1)$ has at most $\frac{p-1}{2}$ roots, hence there are $\frac{p-1}{2}+1=\frac{p+1}{2}$ distinct **quadratic residues** modulo p, or numbers a that have some x such that $x^2\equiv a$mod p.

So some numbers are quadratic residues modulo certain primes, and there are some general case that come up a lot:

1. If $p\equiv 1$mod 4, then -1 is a quadratic residue. If $p\equiv 3$mod 4, then 1 is not a quadratic residue.

2. 2 is a quadratic residue modulo p iff $p\equiv\pm 1(\text{mod }8)$.

3. 3 is a quadratic residue modulo p iff $p\equiv\pm 1(\text{mod }12)$.

Using these cases and similar arguments to the above, many different types of problems can be solved.

Example 2.2

What is the remainder when:

$$\prod_{n=0}^{150}(n^2-2n-2)$$

is divided by 151?

Solution: We note that 151 is prime and is 3 mod 4, so $\prod_{n=0}^{150}(n^2-2n+2)=\prod_{n=0}^{150}(n-1)^2+1\neq 0$, as -1 is not a quadratic residue. Note that this is just $\prod_{n=0}^{150}(n-1)^2+1=((1-1)^2+1)\prod_{x=1}^{150}x^2+1=\prod_{x=1}^{150}x^2+1$. This is just the product of $-(-1-x))^2$, over all non-zero quadratic residues. Since we know the inside to be $(-1)^{\frac{p-1}{2}}-1$, we know the entire expression is just $\boxed{4}$.

§3 Problem Set

Easy Problems

1. Find $ord_7(3)$
2. Find $ord_{1025}(2)$
3. Find $ord_{a^2+1}(a)$ for all integers $a > 1$.
4. Prove that if $k = ord_b(a)$, $a^c \equiv a^{c+k}$ (mod b).
5. For which p is $f(x) : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ that maps $x \longrightarrow x^3$ a bijective map? Why?

Medium Problems

1. Prove that $n \mid \phi(a^n - 1)$ for all a, n. (Saint Petersburg Mathematical Olympiad)
2. How many positive integer multiples of 1001 can be expressed in the form $10^j - 10^i$, where i and j are integers and $0 \le i < j \le 99$? (2011 AIME II 10)
3. Define $\phi^!(n)$ as the product of all positive integers less than or equal to n and relatively prime to n Compute the number of integers $2 \le n \le 50$ such that n divides $\phi^!(n) + 1$.
4. Suppose $P(x)$ is a degree n monic polynomial with integer coefficients such that 2013 divides $P(r)$ for exactly 1000 values of r between 1 and 2013 inclusive. Find the minimum value of n. (PUMAC 7 2013 NT)
5. Find the sum of all possible sums $a + b$ where a and b are nonnegative integers such that $4^a + 2^b + 5$ is a perfect square. (PUMAC 4 2012 NT)

Challenging Problems

1. Find all pairs of prime p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$. (Bulgaria 1996)
2. Let $p = 101$ and let S be the set of p-tuples $(a_1, a_2, ..., a_p) \in \mathbb{Z}_p$ of integers. Let N denote the number of functions $f : S \longrightarrow \{0, 1, ..., p-1\}$ such that $f(a+b)+f(ab) \equiv 2(f(a) + f(b))$mod p for all $a, b \in S$, and $f(a) = f(b)$ whenever all components of ab are divisible by p. Compute the number of positive integer divisors of N. (Here addition and subtraction in $\mathbb{Z}_p$ are done component-wise.) (OMO Fall 2018)
3. The Fibonacci sequence is defined as follows: $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for all integers $n \ge 2$. Find the smallest positive integer m such that $F_m \equiv 0(\text{mod } 127)$ and $F_{m+1} \equiv 1(\text{mod } 127)$. (HMMT Alg/NT 2017 9)
4. Find the remainder when
$$\prod_{i=1}^{2016} (i^4 + 5)$$
is divided by 2017.(USMCA Challenger 24)
5. Find the remainder when
$$\prod_{i=1}^{1903} (2^i + 5)$$
is divided by 1000. (PUMAC 5 2018 NT)