EGMO Training 2017 - Exponents (mod p)

Foundations

1. Let p be a prime number. The following formulae hold for polynomials with coefficients (mod p):

a) **Schoolboy's binomial theorem.** $(X+Y)^p \equiv X^p + Y^p \pmod{p}$.
b) $P(X^p) \equiv (P(X))^p \pmod{p}$ for every polynomial $P(X) \in \mathbb{Z}[X]$.

2. Let p be a positive integer. For another integer a such that $\gcd(a,p) = 1$, there must exist a number $m \in \mathbb{N}$ such that $a^m = 1 \pmod{p}$. The **smallest** such m is called the **order** of $a \pmod{p}$, denoted as $\operatorname{ord}_p a$. The order has the following properties:

a) $a^m = 1 \iff \operatorname{ord}_p a | m$. In particular, $\operatorname{ord}_p a | \varphi(p)$.
b) $\operatorname{ord}_p a^n = \dfrac{\operatorname{ord}_p a}{\gcd(n,\ \operatorname{ord}_p a)}$.
c) For p and q relatively prime, $\operatorname{ord}_{pq} a = \operatorname{lcm}(\operatorname{ord}_p a,\ \operatorname{ord}_q a)$.

3. Let p be a prime number. Then there exists a such that

$$\{1, 2, ..., p-1\} = \{a, a^2, a^3, ..., a^{p-2}, a^{p-1}\} \pmod{p}.$$

Note: the order in which the elements are listed in the two sets above may differ.

Such a number a is called a *primitive* root (mod p). More generally, a number a is called a *primitive* root (mod n) if $\operatorname{ord}_n a = \varphi(n)$.

4. Let p be an odd prime. The equation $x^2 \equiv a$ has solution (mod p) if and only if $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. In this case we say that x is a square mod p.

- $-1 = x^2 \pmod{p} \iff p \equiv 1 \pmod{4}$.
- $+2 = x^2 \pmod{p} \iff p \equiv 1 \text{ or } -1 \pmod{8}$.
- $-2 = x^2 \pmod{p} \iff p \equiv 1 \text{ or } 3 \pmod{8}$.
- $-3 = x^2 \pmod{p} \iff p \equiv 1 \pmod{6}$.

5. Consider the set $\mathbb{Z}[\sqrt{d}] = \{a + \sqrt{d}b\ ;\ a, b \in \mathbb{Z}\}$ and the map $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}$ given by

$$N(a + \sqrt{b}) = |a^2 - db^2|.$$

N is known as a norm on $\mathbb{Z}[\sqrt{d}]$.

a) N is multiplicative:

$$N((x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d})) = N(x_1 + y_1\sqrt{d})N(x_2 + y_2\sqrt{d}).$$

b) For each $d \in \{-2, -1, 1, 2, 3\}$, the norm above is Euclidean: We can divide two elements in $\mathbb{Z}[\sqrt{d}]$ and get a remainder whose norm is less than the norm of the divisor.
c) Unique Prime Factorization does not hold in $\mathbb{Z}[\sqrt{d}]$ for $d < -2$ by using that $2 \neq |x^2 - dy^2|$ for x, y integers, while every integer is a square (mod 2).

Problems

Q1. Using the binomial formula $\sum_{k=0}^{n} \binom{n}{k} X^k = (1+X)^k$ and the Schoolboy's binomial theorem, prove Lucas' Theorem: $\binom{n}{k} \equiv \prod_{i=0}^{d} \binom{n_i}{k_i} \pmod{p}$, where

$n = n_d p^d + n_{d-1} p^{d-1} + \cdots + n_1 p + n_0$, and

$k = k_d p^d + k_{d-1} p^{d-1} + \cdots + k_1 p + k_0$ are the base p expansions of n and k respectively. This uses the convention that $\binom{n}{k} = 0$ if $n < k$.

Write down the first 30 lines of Pascal's triangle (mod 2). Use the above theorem to explain the patterns you observed.

Q2. Find the order of each integer (mod p) when $p = 7, 9, 11$ and 13 respectively. Find the primitive roots in each case.

Q3. Use induction to prove that $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ for every $n > 2$. Hence prove that there are no primitive roots (mod 2^n) for $n > 2$.

Q4. Prove that there are no primitive roots (mod n) if n has two distinct odd prime factors, or an odd prime factor and a factor 2^l with $l > 1$.

Q5. (IMO2005) Determine all positive integers relatively prime to all the terms of the infinite sequence

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

[Hint: For which numbers n does this equation make sense $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1 \pmod{n}$?]

Q6. a) Write the product $(x_1^2 + x_2^2)(y_1^2 + y_2^2)$ as a sum of two squares.
b) Prove that a positive integer n is a sum of two squares iff all primes p satisfying $p \equiv 3 \pmod 4$ have even exponent in the prime factorization of n.

Q7. a) Prove that an odd prime p can be written as $p = x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$ $\iff p \equiv 1$ or $3 \pmod 8$.
b) Prove that a positive integer n can be written as $n = x^2 + 2y^2$ iff all primes p satisfying $p \equiv 5$ or $7 \pmod 8$ have even exponent in the prime factorization of n.

Q8. Let ξ be a complex 3rd or 6th root of 1. Consider the following norm on $\mathbb{Z}[\xi]$:

$$N(a + b\xi) = (a + b\xi)(a + b\xi^2) = a^2 \pm ab + b^2.$$

a) Prove that N is multiplicative: $N((a + b\xi)(c + d\xi)) = N(a + b\xi)N(c + d\xi)$.
b) Prove that $\mathbb{Z}[\xi]$ with the norm above is Euclidean.

Q9. Let p be an odd prime. Prove that p can be written as $p = x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1 \iff p \equiv 1 \pmod 6$.

[Hint: In the equation $u^2 + 3 = 0$ use a change of variables $u = 2t - 1$ and use the previous question.]