PUTNAM TRAINING - NUMBER THEORY

THOMAS HALES

1. WHAT YEAR IS IT?

2017 is the 306th prime. In binary 2017 = $1111100001_2$.

$2017 = 44^2 + 9^2 = 11^3 + 7^3 + 7^3$

2. REFERENCES FOR NUMBER THEORY

- Chapter 5 of Putnam and Beyond, by Gelca and Andreescu
- A Classical Introduction to Modern Number Theory, 2nd edition, by Ireland and Rosen, chapters 1 (factorization), 2 (arithmetic functions), 3 (congruence), 5 (quadratic reciprocity), 7 (finite fields), 10 (equations over finite fields), 12 (number fields), 17 (Diophantine equations).

3. SOME PAST PUTNAM PROBLEMS RELATED TO NUMBER THEORY


4. GREATEST COMMON DIVISOR

The greatest common divisor $d = \gcd(a, b)$ of $a, b \in \mathbb{Z}$ has the following properties.

Date: 2017.
It can be quickly computed by the Euclidean algorithm.
- It is the least positive \( d \) of the form \( xa + yb \), with \( x, y \in \mathbb{Z} \).
- The \( x \) and \( y \) can be quickly computed by the extended Euclidean algorithm.

We say that \( a \) and \( b \) are relatively prime if \( \gcd(a, b) = 1 \).

5. ARITHMETICAL FUNCTIONS

Let \( n = p_1^{a_1} \cdots p_k^{a_k} \) be the prime factorization of the positive integer \( n \).

Let \( \nu(n) \) be the number of positive divisors of \( n \).

\[
\nu(n) = (a_1 + 1) \cdots (a_k + 1).
\]

Example, \( \nu(2016) = \nu(2^3 \cdot 3^1 \cdot 7^1) = 6 \cdot 3 \cdot 2 = 36 \).

Let \( \sigma(n) \) be the sum of the positive divisors of \( n \).

\[
\sigma(n) = \sigma(p_1^{a_1}) \cdots \sigma(p_k^{a_k}), \quad \sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}.
\]

Let \( \phi(n) \) (Euler totient function) be the number of integers \( 1 \leq k \leq n \) that are relatively prime to \( n \).

\[
\phi(n) = n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k).
\]

For example \( \phi(3^4 \cdot 5^2) = 3^4 \cdot 5^2(2/3)(4/5) \).

Let \( \mu(n) \) be \((-1)^k\) if \( n \) is the product of \( k \) distinct prime factors, and \( \mu(n) = 0 \) otherwise.

Write \( a \mid b \) to mean that \( a \) divides \( b \).
The M"obius inversion formula states that
\[ F(n) = \sum_{d|n} f(d) \implies f(n) = \sum_{d|n} \mu(d) F(n/d). \]

6. CONGRUENCE

Let \( a, b, m \in \mathbb{Z} \) and \( m \neq 0 \). We write
\[ a \equiv b \pmod{m} \]
to mean that \( m \) divides \( a - b \).

Congruence is an equivalence relation (that is, it is reflexive, symmetric, and transitive).

If \( 1 = \gcd(a, n) \), then \( ax \equiv b \pmod{n} \) has a unique solution \( x \mod{n} \). In particular, if \( n = p \) a prime, then \( ax \equiv b \pmod{p} \) has a unique solution \( x \mod{p} \), unless \( p | a \). (This means that arithmetic modulo a prime is a field.)

Fermat's little theorem states that if \( a \) and \( p \) are relatively prime, with \( p \) prime, then
\[ a^{p-1} \equiv 1 \pmod{p}. \]

Also, for all \( a \),
\[ a^p \equiv a \pmod{p}. \]

More generally, Euler's theorem states that if \( \gcd(a, m) = 1 \), then
\[ a^{\phi(m)} \equiv 1 \pmod{m}. \]

Wilson's theorem states that if \( p \) is a prime, then
\[ (p - 1)! \equiv -1 \pmod{p}. \]

The Chinese remainder theorem states that if \( m \) and \( n \) are relatively prime, then the system of congruences
\[ x \equiv a \pmod{m}, \]
\[ x \equiv b \pmod{n}, \]
has a unique solution in \( x \mod{mn} \). (This generalizes to a system of \( k \) congruence equations \( x \equiv a_i \pmod{m_i} \), provided that \( \gcd(m_i, m_j) = 1 \), for all \( i \neq j \).

To find all solutions to an equation \( x \equiv c \pmod{n} \), where \( n = p_1^{a_1} \cdots p_k^{a_k} \), find all the solutions \( x \equiv c_i \pmod{p_i^{a_i}} \) for each \( i \), then combine the results using the Chinese Remainder theorem.
A quadratic equation
\[ ax^2 + bx + c \equiv 0 \pmod{p} \]
has solutions given by the quadratic equation, provided that \( p \neq 2 \) is a prime. If \( b^2 - 4ac \) is not a square, then the quadratic equation has no roots.

If \( f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0 \) is a polynomial of degree \( k \), then
\[ f(x) \equiv 0 \pmod{p}, \]
has at most \( k \) roots, counted with multiplicities.

7. SOME PROBLEMS

7.1. from from Ireland and Rosen. (1.30) Prove that
\[ 1/2 + 1/3 + \cdots + 1/n \]
is not an integer.

(1.28) Show that
\[ n^7 \equiv n \pmod{42}. \]

(2.10) A function on the integers is said to be multiplicative if \( f(ab) = f(a)f(b) \), whenever \( \gcd(a, b) = 1 \). If \( f(n) \) is a multiplicative function, show that
\[ g(n) = \sum_{d|n} f(d) \]
is also multiplicative.

(2.17) Show that \( \sigma(n) \) is odd iff \( n \) is a square or twice a square.

(2.20) Show that
\[ \prod_{d|n} d = n^{\mu(n)/2}. \]

(2.22) Show that the sum of all the integers \( t \) such that \( 1 \leq t \leq n \) and \( \gcd(t, n) = 1 \) is \( n\phi(n)/2 \).

(3.10) Find all positive integers \( n > 1 \) such that
\[ (n - 1)! \not\equiv 0 \pmod{n}. \]
(3.15) For any prime \( p \) show that the numerator of \( 1 + 1/2 + 1/3 + \cdots + 1/(p - 1) \) is divisible by \( p \).

(4.18) Find all solutions to the equation
\[
1 + x + x^2 + \cdots + x^b = 0 \mod 29.
\]

(4.22) If \( a \) has order 3 modulo \( p \), show that \( 1 + a \) has order 6.

8. Successive approximations

Suppose that \( f \) is a polynomial and that \( x_0 \) satisfies
\[
f(x_0) \equiv 0 \mod p^k.
\]

To solve the equation modulo \( p^{k+1} \), try \( x_0 + p^k x \) for some \( x \). Then setting \( f(x_0) = p^k h \), we have
\[
f(x_0 + p^k x) = f(x_0) + f'(x_0) p^k x \equiv p^k(h + f'(x_0)x) \equiv 0 \mod p^{k+1}
\]

provided \( x \) is a solution to the linear equation
\[
h + f'(x_0)x \mod p.
\]

Example: solve Putnam 1986-B3.

9. Points on a conic section

Working in a field, we can solve for the general solution to the equation
\[
a x^2 + b xy + c y^2 + d x + e y + f = 0,
\]
once a particular solution \((x, y) = (x_0, y_0)\) is known. The method is to write a parametric equation of a line \( t \mapsto (x_0 + t \lambda, y_0 + t \mu) = (x, y) \), where \((\lambda, \mu)\) are fixed constants that determine the slope of the line. We substitute this formula for \((x, y)\) into the equation of the conic and solve the quadratic equation for \( t \). One of the roots of the quadratic equation is \( t = 0 \), we obtain a linear equation for \( t \).

Putnam 1991-B5. Working in \( \mathbb{F}_p \), count the cardinality of the set
\[
\{x^2 \mid x \in \mathbb{F}_p\} \cap \{y^2 + 1 \mid y \in \mathbb{F}_p\}.
\]
Putnam 1987-B4. Let $F$ be a field where $1 + 1 \neq 0$. Show that the general solution to $x^2 + y^2 = 1$ has the form

$$(x, y) = \left( \frac{r^2 - 1}{r^2 + 1}, \frac{2r}{r^2 + 1} \right),$$

or $(x, y) = (1, 0)$, where $r^2 \neq -1$.

10. **Pell's equation**

Pell’s equation is

$$x^2 - Dy^2 = 1,$$

where $D$ is positive and not a square.

If $(x_1, y_1)$ and $(x_2, y_2)$ are solutions of Pell’s equation then $(x_3, y_3)$ is also a solution, where

$$x_3 + y_3 \sqrt{D} = (x_1 + y_1 \sqrt{D})(x_2 + y_2 \sqrt{D}).$$

One way to solve Pell’s equation is with the continued fraction approximations of $\sqrt{D}$.

Problem: find the continued fraction of $\sqrt{3}$. Use it to find solutions to Pell’s equation for $D = 3$.

11. **Solutions to multivariate equations of degree 3 and higher**

There is no general method. Look for special properties of the equation.

12. **Diophantine equations**

Diophantine equations deal with solutions to polynomial equations in the integers.

The simplest case is a linear equation

$$ax + by = c,$$
for fixed constants $a, b, c$. Let $d = \gcd(a, b)$. Then $d$ divides the left-hand side, so $d$ must divide the right hand side if there are any solutions: $c \equiv 0 \mod d$. Write $a = a'd$, $b = b'd$, $c = c'd$. Then the linear equation reduces to

$$a'x + b'y = c',$$

where $\gcd(a', b') = 1$.

Find all integer solutions to $3x + 4y = 5$ by solving mod 4 for $x$.

13. Descent

Show that the equations have no solution:

$$x^2 + 5y^2 = \varepsilon^2$$

$$5x^2 + y^2 = \rho^2.$$