Number Theory: definitions and theorems

October 27, 2019

- Euler totient function: for $n \in N$: $\phi(n) = \#\{k \in N \mid 1 \leq k \leq n;\ gcd(n,k) = 1\}$.
  - Euler's theorem: for any $n \in N$ and $a \in Z$ such that $gcd(a,n) = 1$: $a^{\phi(n)} \equiv 1 \pmod{n}$.
  - If n and m are coprime positive integers then $\phi(nm) = \phi(n) \cdot \phi(m)$
  - If $n = \prod\limits_{i=1}^{k} p_i^{\alpha_i}$ where p_i are distinct primes then $\phi(n) = n \cdot \prod\limits_{i=1}^{k} (1 - \frac{1}{p_i})$.
  - If n is prime then $\phi(n) = n - 1$ and Euler's theorem is called Fermat's little theorem.
- Let p be odd prime. Nonzero number a is called "quadratic residue" modulo p if there exists number x such that $a \equiv x^2 \pmod{p}$. Otherwise a is called "quadratic nonresidue" modulo p.
  - There are exactly $\frac{p-1}{2}$ quadratic residues modulo p and as many quadratic nonresidues.
  - The product of two quadratic residues is also quadratic residue. The product of quadratic residue and quadratic nonresidue is quadratic nonresidue. The product of two quadratic nonresidues is quadratic residue.
  - If a is quadratic residue then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Otherwise $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
  - -1 is quadratic residue if and only if $p \equiv 1 \pmod{4}$.
- "Legendre symbol" (or "quadratic character"):

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \text{ divides } a \\ 1 & \text{if } a \text{ is quadratic residue modulo } p \\ -1 & \text{if } a \text{ is quadratic nonresidue modulo } p \end{cases}$$

  - $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
  - Gauss quadratic reciprocity: if p and q are distinct odd primes then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.
- Number g is called "generator" or "primitive root" modulo m if $gcd(g,m) = 1$ and all the numbers $g^1, g^2, \ldots, g^{\phi(m)}$ are distinct modulo m.
  - g is generator if $gcd(g,m) = 1$ and $\phi(m)$ is the smallest number $k \in N$ such that $g^k = 1$ (such smallest k for number a is called "multiplicative order of a modulo m".
  - If $gcd(a,m) = 1$ then there exists positive integer k such that $g^k \equiv a \pmod{m}$.
  - Generator exists for modulo $m \Leftrightarrow m = 2$ or $m = 4$ or $m = p^k$ or $m = 2p^k$ where k is positive integer and p is odd prime (In particular, generator exists for any prime number).
  - If there exists a generator modulo m then there are exactly $\phi(\phi(m))$ generators modulo m.
- Some other useful facts.
  - Lifting the exponent lemma. Let us say $p^k \parallel a$ if $p^k \mid a$ and $p^{k+1} \nmid a$.
    Let $p^t \parallel a - 1$ and $p^k \parallel n$. If $p = 2$, $t = 1$ and $k \geq 1$ then $2^{k+2} \mid a^n - 1$. And if $p \geq 3$ or (!!!) $t \geq 2$ then $p^{t+k} \parallel a^n - 1$ (even if $k = 0$).
  - Wilson's theorem. p is prime $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$.
  - Bertrand's postulate. For every integer $n \geq 4$ there exists prime number p such that $n < p < 2n - 2$.
  - Dirichlet's prime number theorem. For any two positive coprime integers a and d, there are infinitely many primes of the form $a + nd$, where n is also a positive integer.