

Number theory quick reference

Paul Dumais, October 2002

1 NOTATIONS.

$$\begin{aligned}\mathbb{P} &= \{p \in \mathbb{N} : p \text{ is prime}\} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots\}, \\ \mathbb{Z}_n &= \{0, 1, \dots, n-1\}, \\ \mathbb{Z}_n^* &= \{x \in \mathbb{Z}_n : \gcd(x, n) = 1\}.\end{aligned}$$

2 DEFINITION (group). A set G together with an operation \circ defined on G is a *group* if the following axioms are satisfied:

- (*associativity*) $\forall x, y, z \in G : (x \circ y) \circ z = x \circ (y \circ z)$,
- (*neutral element*) $\exists e \in G : \forall x \in G : e \circ x = x \circ e = x$,
- (*inverses*) $\forall x \in G : \exists x' \in G : x \circ x' = x' \circ x = e$.

The group is *commutative* if:

$$\forall x, y \in G : x \circ y = y \circ x.$$

The finite group G is *cyclic* if:

$$\exists \alpha \in G : G = \{e, \alpha, \alpha \circ \alpha, \alpha \circ \alpha \circ \alpha, \dots, \underbrace{\alpha \circ \dots \circ \alpha}_{|G|-1 \text{ times}}\},$$

and α is called a *generator* of G . Note that if G is cyclic then G is commutative.

3 THEOREMS.

The set \mathbb{Z}_n is a cyclic group with respect to addition mod n .

The set \mathbb{Z}_n^* is a commutative group with respect to multiplication mod n .

If $p \in \mathbb{P}$, then \mathbb{Z}_p^* is a cyclic group with respect to multiplication mod p .

4 DEFINITION (Euler function).

$$\phi(n) \stackrel{\text{def}}{=} |\mathbb{Z}_n^*|.$$

5 THEOREM (Lagrange).

$$\forall n \geq 1, \forall x \in \mathbb{Z}_n^* : x^{\phi(n)} \bmod n = 1.$$

6 DEFINITIONS (*quadratic residues and quadratic non-residues*).

$$Q_n \stackrel{\text{def}}{=} \{x \in \mathbb{Z}_n^* : (\exists z \in \mathbb{Z}_n^* : z^2 \bmod n = x)\},$$

$$\bar{Q}_n \stackrel{\text{def}}{=} \mathbb{Z}_n^* \setminus Q_n.$$

If $x \in Q_n$ then x is called a *quadratic residue mod* n . If $x \in \bar{Q}_n$ then x is called a *quadratic non-residue mod* n .

7 THEOREM (*Euler's criterion*). Let $p \in \mathbb{P}$ be odd, then:

$$a \in Q_p \iff a^{\frac{p-1}{2}} \bmod p = 1.$$

8 DEFINITIONS (*Legendre and Jacobi symbols*).

Let $p \in \mathbb{P}$ be odd and let $a \in \mathbb{Z}$, then the *Legendre symbol* of a and p is:

$$\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{if } a \bmod p = 0 \\ 1 & \text{if } a \bmod p \in Q_p \\ -1 & \text{if } a \bmod p \in \bar{Q}_p \end{cases}.$$

Let $n \geq 3$ be odd and let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ be the prime factorization of n . Let $a \in \mathbb{Z}$. The *Jacobi symbol* of a and n is:

$$\left(\frac{a}{n}\right) \stackrel{\text{def}}{=} \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}.$$

9 THEOREM (*Chinese remainder theorem*). Let m_1, m_2, \dots, m_r be pairwise relatively prime positive integers, and let $a_1, a_2, \dots, a_r \in \mathbb{Z}$. Then the system of r congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

has a unique solution modulo $M = m_1 m_2 \dots m_r$, given by

$$x = \sum_{i=1}^r a_i M_i y_i \bmod M,$$

where $M_i = M/m_i$ and $y_i = M_i^{-1} \bmod m_i$.