1 The Division Algorithm

Theorem 1.1. *For integers a, b, and c, if $a \mid b$ and $a \mid c$, then $a \mid b + c$.*

Theorem 1.2. *For integers a, b, and c, if $a \mid b$ and $a \mid c$, then $a \mid b - c$.*

Theorem 1.3. *For integers a, b, and c, if $a \mid b$ and $a \mid c$, then $a \mid bc$.*

Theorem 1.4. *For integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

Theorem 1.5. *For a natural number n, congruence modulo n is reflexive, symmetric, and transitive*

Theorem 1.6. *For integer a, b, c, d and a natural number n, if $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$.*

Theorem 1.7. *For integer a,b,c,d and a natural number n, if $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a - c \equiv b - d \mod n$.*

Theorem 1.8. *For integer a, b and natural numbers n, m if $a \equiv b \mod n$ and then $ma \equiv mb \mod mn$.*

Theorem 1.9. *For integer a, b, c, d and a natural number n, if $a \equiv b \mod n$ and $c \equiv d \mod n$, then $ac \equiv bd \mod n$.*

Theorem 1.10. *For integer a, b and a natural number n, $a \equiv b \mod n$ if and only if a and b have the same remainder when divided by n.*

Theorem 1.11. *For integers a, b, n, r and k, if $a \equiv nb + r$, $k \mid a$ and $k \mid b$, then $k \mid r$.*

Theorem 1.12. *For integers a, b, n and r, if $a = nb + r$ then $\gcd(a, b) = \gcd(b, r)$.*

Theorem 1.13. *For integers a, b and d, the diophantine equation $ax + by = d$ has a solution (with x and y integers) if and only if $\gcd(a, b) \mid d$.*

Corollary *For integers a and b, the diophantine equation $ax + by = 1$ has a solution (with x and y integers) if and only if $\gcd(a, b) = 1$.*

Theorem 1.14. *For integers a and b, if x' and y' are integral solutions to the diophantine equation $ax + by = d$, then all solutions are given by*

$$x = x' + \frac{b}{\gcd(a, b)}t \qquad y = y' - \frac{a}{\gcd(a, b)}t$$

where t is an integer.

Theorem 1.15. *For integers a, b, c and a natural number n, if $ac \equiv bc \mod n$ and $\gcd(c, n) = 1$, then $a \equiv b \mod n$.*

2 Theorems About Primes

Theorem 2.1. *A natural number n is prime if and only if for all $p < \sqrt{n}$, p does not divide n.*

Fundamental Theorem of Arithmetic *Every natural number greater than 1 is either a prime number or it can be expressed uniquely as a product of primes.*

Theorem 2.2. *For natural numbers a and b, if $a^2 \mid b^2$ then $a \mid b$.*

Theorem 2.3. *For natural numbers a, b and n, if $a \mid n$, $b \mid n$ and $\gcd(a, b) = 1$ then $ab \mid n$.*

Theorem 2.4. *For p pries and integers a and b, if $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Lemma *For any $n \in \mathbb{N}$, $\gcd(n, n + 1) = 1$.*

Theorem 2.5. *There are infinitely many primes.*

3 Theorems About Modularity

Theorem 3.1. *For a polynomial* $f(x) = a_k x^k + a_{k-1} x^{k-1} + ... + a_1 x + a_0$, *if* $a \equiv b \mod n$ *then* $f(a) \equiv f(b) \mod n$.

Theorem 3.2. *For an integer* a *and natural number* n, *there is a unique integer* t *in* $\{0, 1, ..., n-1\}$ *such that* $a \equiv t \mod n$.

Theorem 3.3. *For integers* a, b, n *with* $n > 0$, $ax \equiv b \mod n$ *has a solution if and only if there exist integers* x *and* y *such that* $ax + ny = b$.

Theorem 3.4. *For integers* a, b, n *with* $n > 0$, $ax \equiv b \mod n$ *has a solution if and only if* $\gcd(a, n) \mid b$.

Theorem 3.5. *For integers* a, b, n *with* $n > 0$, *if* x' *is a solution to* $ax \equiv b \mod n$, *then all solutions are given by*

$$x' + \frac{n}{\gcd(a, n)} m \mod n$$

where $m = 0, 1, ..., \gcd(a, n) - 1$.

Chinese Remainder Theorem Let $n_1, n_2, ..., n_r$ be positive integers such that $(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_r \mod n_r \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $N = n_1 \cdot n_2 \cdot ... \cdot n_r$.

4 Higher Degree Congruences

Theorem 4.1. *For natural numbers* a *and* n *there exists natural numbers* i *and* j *with* $i \neq j$ *such that* $a^i \equiv a^j \mod n$.

Theorem 4.2. *For natural numbers* a *and* n *if* $\gcd(a, n) = 1$ *then there exists a natural number* k *such that* $a^k \equiv 1 \mod n$.

Theorem 4.3. *For natural numbers* a *and* n, *with* $\gcd(a, n) = 1$ *and* $ord_n(a) = k$, *then* $a^m \equiv 1 \mod n$ *if and only if* $k \mid m$.

Theorem 4.4. *For a prime* p *and natural number* m, $\Phi(p^m) = p^m - p^{m-1}$.

Fermat's Little Theorem For p prime, and $\gcd(a, p) = 1$, $a^{p-1} \equiv 1 \mod p$.

Euler's Theorem For integers a and n, with $n > 0$ and $\gcd(a, n) = 1$, $a^\Phi(n) \equiv 1 \mod n$.

Wilson's Theorem For a natural number n, $(n-1)! \equiv -1 \mod n$ if and only if n is prime.

5 Cryptography

Theorem 5.1. *If p and q are primes and W is a natural number less than p, q then $W^{(p-1)(q-1)} \equiv 1 \mod pq$.*

Theorem 5.2. *If p and q are primes and W is a natural number less than p, q then $W^{1+(p-1)(q-1)} \equiv W \mod pq$.*

Theorem 5.3. *If p and q are primes and E is a natural number relatively prime to $(p-1)(q-1)$, then there exist natural numbers D and y such that $ED = 1 + y(p-1)(q-1)$.*

Theorem 5.4. *If p and q are primes and W is a natural number less than p, q and $ED = 1+y(p-1)(q-1)$ then $W^{ED} \equiv W \mod pq$.*

6 Primitive roots and high order congruences

Theorem 6.1. *Suppose p is prime, $ord_p(a) = d$ and $\gcd(i, d) = 1$, then $ord_p(a^i) = d$.*

Lagrange's Theorem If p is prime and $f(x)$ is a degree n polynomial then $f(x) \equiv 1 \mod p$ has at most n incongruent solutions modulo p.

Theorem 6.2. *For a prime p and a natural number n, there are at most $\Phi(d)$ many incongruent integers modulo p that have order d modulo p.*

Theorem 6.3. *For a prime p and a primitive root g, the set $\{0, g, ..., g^{p-1}\}$ is a complete residue system modulo p.*

Theorem 6.4. *For any natural number n, $\sum \Phi(d) = n$ where the sum is take over the divisors d of n.*

Theorem 6.5. *Every prime p has a primitive root.*

Theorem 6.6. *For natural numbers k, b and an integer n, with $\gcd(k, \Phi(n)) = 1$ and $\gcd(b, n) = 1$, then the congruence*

$$x^k \equiv b \mod n$$

has a unique solution modulo n given by

$$x \equiv b^u \mod n$$

where u is a solution to the diophantine equation $ku + \Phi(n)v = 1$.