Greatest Common Divisor

1. **Proposition 2.15** Let a, b, q be integers. Then $\gcd(a, b) = \gcd(a, b - aq)$
2. **Proposition 2.19** Let a, b, c be integers such that $\gcd(a, c) = 1$. Then $\gcd(c, ab) = \gcd(c, b)$.
3. **Corollary 2.20** Let a, b, c be integers. Suppose $c \mid ab$ and $\gcd(a, c) = 1$. Then $c \mid b$
4. **Euclid's Lemma** (Pls remember it exists) If p prime then if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Distribution of Primes

1. List of prime numbers

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997		

Table 1: Primes from 1 to 1000

2. Key Identity $\rightarrow 2^n \leq L_n \leq 4^{n-1}$

3. **Legrende Formula**:

$$\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor = \sum_{k=1}^{\lfloor \log_p n \rfloor} \lfloor \frac{n}{p^k} \rfloor = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots$$

4. **Lemma 4.5** Let p be a prime and let $n = 1, \cdots, p-1$. Then $\nu_p(\binom{p}{n}) = 1$

$$\nu_p(\binom{p}{n}) = \lfloor \frac{p}{p} \rfloor - \lfloor \frac{n}{p} \rfloor - \lfloor \frac{p-r}{p} \rfloor = 1 - 0 - 0 = 1$$

5.

$$\lfloor \frac{n}{a} \rfloor - \lfloor \frac{m}{a} \rfloor - \lfloor \frac{n-m}{a} \rfloor = \begin{cases} 1 & \text{if } n\%a \leq m\%a \\ 0 & \text{if } n\%a \geq m\%a \end{cases}$$

6. **LTE (p is odd)** If $p \nmid a$ and $p \nmid b$ with $p \mid a - b$. Then:

$$\nu_p(a^n - b^n) = \nu_p(a+b) + \nu_p(n)$$

7. **LTE (p is even)** If a, b are odd and n is even, then:

$$\nu_2(a^n - b^n) = \nu_2(a^2 + b^2) + \nu_2(n) - 1$$

8. Cool technique I learned while practicing:

$$10! = \frac{\frac{10!}{5! \cdot 5!}}{\frac{5!}{2! \cdot 3!} \cdot \frac{5!}{2! \cdot 3!}} \over 2! \cdot 3! \cdot 2! \cdot 3!$$

Cyclotomic Polynomials

1. $\Phi_1(x) = x - 1$
   $\Phi_2(x) = x + 1$
   $\Phi_3(x) = x^2 + x + 1$
   $\Phi_4(x) = x^2 + 1$
   $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
   $\Phi_6(x) = x^2 - x + 1$
   $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
   $\Phi_8(x) = x^4 + 1$
   $\Phi_9(x) = x^6 + x^3 + 1$
   $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$
   $\Phi_{11}(x) =$ too long but you should know
   $\Phi_{12}(x) = x^4 - x^2 + 1$

2. **Exercise 5.1** Euler Trotient ϕ properties:

   (a) $\phi(1) = 1$, $\phi(p) = p - 1$ for prime p

   (b) $\phi(m) = 2$ iff $m = 3, 4, 6$.

   (c) $\phi(p^k) = p^k - p^{k-1}$

   (d) $\phi(mn) = \phi(m) \cdot \phi(n)$ if m and n are co-prime integers

3. $x^m - 1 = \prod_{d|m} \Phi_d(x) \rightarrow$ If p prime, $\Phi_p(x) = \frac{x^p - 1}{x - 1}$

4. HW4Q1d

   (a) Let p be prime. If $p \nmid \Phi_p(a)$, then $\Phi_p(a) \equiv 1 \pmod{p}$.

   (b) If $m \geq 2$

   $$\Phi_m(1) = \begin{cases} q & \text{if } m = q^k \text{ for some prime } p \\ 1 & \text{otherwise} \end{cases}$$

5. **Proposition 6.8** Let $m \in \mathbb{N}$ and $n > 1$ coprime to m. Then $n \mid \Phi_m(a) \implies o_n(a) = m$

6. **Corollary 6.9** Let p be prime. If $p \mid \Phi_m(a)$, then $p \mid m$ or $p \equiv 1 \pmod{m}$ (because FLT forces it that $m \mid p - 1$).

7. For $m \geq 1$, then $\Phi_m(a) \equiv 1 \pmod{a}$. (Because all cyclotonic polynomials end with a constant 1)

8. Let p be prime, if $p \mid \Phi_p(a)$, then $\nu_p(\Phi_p(a)) = 1 \implies \nu(\Phi_p(a)) \leq 1$ for any a.

9. Let m be odd. We get that $\Phi_m(-x) = \Phi_{2m}(x)$.

Abstract Algebra

1. In case, you met a problem for some reason on additive order in a ring; pls check HW5 Q1
2. A non-zero non-unit element $r \in R$ is said to be
   (a) **irreducible** if it cannot be written as $r = ab$ where a and b are not units
   (b) **prime** if whenever $r \mid ab$ in R for some $a, b \in R$, we have $r \mid a$ or $r \mid b$
3. **CRT**: Let $m, n \geq 2$ be co-prime integers. Then
$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
4. An ideal I of R satisfies these properties:
   (a) $0 \in I$
   (b) for any $a, b \in I$, we have $a + b \in I$
   (c) for any $a \in I$, and any $r \in R$, we have $ra \in I$
5. **Lemma 8.5** If an ideal I of R contains a unit, then $I = R$.
6. **Corollary 8.14** If R is a field, then any $\varphi : R \to S$ is injective.
7. **Theorem 8.19 (First Isomorphim Theorem)** Let $\varphi : R \to S$ be a ring homomorphism. Then the natural map $\psi : R/\ker(\varphi) \to im(\varphi)$ sending the coset $[a]$ to $\varphi(a)$ is an isomorphism.
8. HW6 3
   (a) A proper ideal I is a prime ideal if for any $a, b \in R$, if $I \mid ab$, then $I \mid a$ or $I \mid b$.
   (b) I is a prime ideal of R iff R/I is an integral domain.
   (c) Let S be a subring of R and let I be a prime ideal of R. $S \cap I$ is a prime ideal of S.
9. **HW7 Q3** Let F be a field of char p and let m be where $p \nmid m$.
   (a) if $a \in F^\times$ satisfies $\Phi_m(a) = 0$ then $o(a) = m$
   (b) if $a \in F^\times$ satisfies $o(a) = m$, then $\Phi_m(a) = 0$ and $\Phi'_m(a) = 0$.

Polynomial Ring

1. **Division Algorithmn for Polynomials** Let R be a com ring. Let $f(x) \in R[x]$ and let $g(x) \in R[x]$. If the leading coefficient is the a unit in R then $\exists q(x), r(x) \in R[x]$ s.t.

$$f(x) = g(x)q(x) + r(x) \text{ and } \deg(r) < \deg(g)$$

2. **Props 9.5** A homomorphism $R[x] \to S$ is the same as $R[x] \to R \to S$ with $R[x] \to R$ being an evaluation homorphism of $f(\alpha)$ for $f(x) \in R[x]$.

3. **Corollary 9.7** Let R be an integral domain. $f(x) \in R[x]$ and $c_1, \cdots, c_n$ be distinct then they are roots iff $(x - c_1) \cdots (x - c_n) \mid f(x)$.

4. **Lemma 9.10 (Fropbenius Map)** Let R be a com ring with *charp*. Then the map $r \mapsto r^p$ is a ring homomorphism. In other words,

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$

5. **Proposition 9.12** c is a repeated root of $f(x)$ iff $f(c) = f'(c) = 0$.

6. **HW8 Q3** If $f(x) \in F[x]$ is a monic polynomial so that $f(x) = (x - a_1) \cdots (x - a_n)$ with roots in F (it splits completely). Then its discrimnant is defined as:

$$\Delta(f) = \prod_{1 \le i \le j \le n} (a_i - a_j)^2$$

Finite Fields

1. **Props 9.16** If F is a finite field and let $g(x) \in F[x]$ with deg ≥ 1. Then, the following are equiv:
   (a) $g(x)$ is irreducible
   (b) $F[x]/(g(x))$ is a field
   (c) $F[x]/(g(x))$ is an integral domain
2. **Lemma 9.18** Let F be a field. Let $g(x) \in F[x]$ be a polynomial of deg ≥ 1 then $|F[x]/g(x)| = |F|^d$.
3. **Props 9.18** Let $g(x) \in \mathbb{F}_p[x]$ be a polynomial. Let R be a com ring with char p. Then $\mathbb{F}_p[x]/g(x) \to R$ is the same as giving a root β of $g(x)$ in R
4. **Theorem 9.23** Let p be prime and let $n \in \mathbb{N}$. Then $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where $d \mid n$
5. **From Proof of Theorem 9.23** Let $S_p(n)$ denote he set of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree n. Then
$$n \cdot |S_p(n)| = \sum_{d|m} \mu(d) p^{n/d}$$
   A thing to note is that $p \mid |S_p(n)|$.
6. **Theorem 10.1**
   (a) Every finite field has order p^d for some p and positive integer d. (basically also imples $\mathbb{F}_p^d$ has char p)
   (b) Any two finite fields of the same order are isomorphic
   (c) For every prime p and every positive int d, there is a $g(x) \in \mathbb{F}_p[x]$ irreducible of degree d. In other words, $\mathbb{F}_{p^d} \cong \mathbb{F}_p[x]/(g(x))$
   (d) There exists a homomorphism $\mathbb{F}_{p_1^{d_1}} \to \mathbb{F}_{p_2^{d_2}}$ iff $p_1 = p_2$ and $d_1 \mid d_2$
7. **Theorem 10.7 (Existence of primitive element)** Let F be a finite field, then there is a $\alpha \in F^\times$ where $o(a) = |F| - 1$.
8. Result from Proof of Theoreom 10.7 $\to$ Let F be a field of q elements. For $d \mid q-1$, let N_d denote the number of elements in F with order d. $N_d = \phi(d)$.
9. **Corollary 10.10** Let F be a field of order p^n and positive int n. Then $\alpha \in F$ is in $\mathbb{F}_p$ iff $\alpha^p = \alpha$. (Because $x^p - x$ has all the roots in $\mathbb{F}_p$)
10. **Example 10.11** If $a \in \mathbb{F}_{p^2}$, we have $a^{p+1} \in \mathbb{F}_p$ because $a^{p^2} \cdot a^p = (a^p \cdot a)^p$ and $a^{p^2} = a$.
11. **Lemma 10.14** Let p be a prime, not dividing $m \in \mathbb{N}$. Let $\alpha \in \mathbb{F}_{p^2}^\times$ with $o(\alpha) = m$. Then $\alpha + \alpha^{-1} \in \mathbb{F}_p^\times$ iff $p \equiv \pm 1 \pmod{m}$.

Quadratic Reciprocity

1. **Theoreom 11.4 (Quadratic Reciprocity)**

   (a) Let p be an odd prime for $(a \in \mathbb{F}_p)^\times$. Then:

   $$a^{(p-1)/2} = \begin{cases} 1 \pmod p & \text{if there is an integer x such that } x^2 \equiv a \pmod p \\ -1 \pmod p & \text{if there is no such integer} \end{cases}$$

   (b) -1 is a quadratic residue $\pmod p$ iff $p = 2$ or $p \equiv 1 \pmod 4$. In other words, for $p \neq 2$,

   $$(\frac{-1}{p}) = (-1)^{(p^2-1)/2}$$

   (c) 2 is a quadratic residue mod p iff $p = 2$ or $p \equiv \pm 1 \pmod 8$. In other words, for $p \neq 2$,

   $$(\frac{2}{p}) = (-1)^{(p^2-1)/8}$$

   (d) If p, q are distinct odd primes, then

   $$(\frac{p}{q}) = -(\frac{q}{p}) \text{ if both p,q} \equiv 3 \pmod 4$$
   $$(\frac{p}{q}) = -(\frac{q}{p}) \text{ otherwise}$$

2. **Corollary 11.8** We have

   (a) 3 is a quadratic residue *modp* iff $p = 3$ or $p \equiv \pm 1 \pmod{12}$

   (b) (Extra from HW9 Q1) -3 is a quadratic resdue *modp* iff $p = 2$ or $p = 3$ or $p \equiv 1 \pmod 3$.

   (c) 5 is a quadratic residue *modp* iff $p = 5$ or $p \equiv \pm 1, \pm 9 \pmod{20}$

   (d) 7 is a quadratic residue *modp* iff $p = 7$ or $p \equiv \pm 1, \pm 9, \pm 25 \pmod{28}$

3. **Theorem 11.13 (Hensel's Lemma)** Let p be a prime. Let $f(x) \in \mathbb{Z}_p[x]$ and $r \in \mathbb{Z}_p$. Suppose

   $$\nu_p(f(r)) > 2\nu_p(f'(r))$$

   Then there exists $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\nu_p(a - r) > \nu_p(f(r)) - \nu_p(f'(r))$.

4. **Corollary 11.16 (Nooby Hensel's Lemma)** Suppose $f(x) \in \mathbb{Z}[x]$. Let p be a prime and let $r \in \mathbb{F}_p$. Suppose $f(r) = 0$ and $f'(r) \neq 0$ in $\mathbb{F}_p$. Then there exists $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$.

5. **Jacobi Symbol Def** (Just there in case) Given two coprime integers a, b where b is a positive odd integer, we factor $b = p_1 \cdots p_r$ into a product of (possibly equal) odd primes. Then we define the Jacobi symbol

   $$\left(\frac{a}{b}\right) := \prod_{j=1}^{r} \left(\frac{a}{p_j}\right).$$

6. **Theorem 11.20 (Quadratic Reciprocity for Jacobi Symbols)** Let b be a positive odd integer. Then:

   (a) $(\frac{-1}{b}) = (-1)^{(b-1)/2}$

   (b) $(\frac{2}{b}) = (-1)^{(b^2-1)/8}$

   (c) if a is a positive odd integer co-prime to b, then $(\frac{a}{b})(\frac{b}{a}) = (-1)^{(a-1)(b-1)/4}$

Group Theory

1. **Theorem 12.3 (Lagrange's Theorem)** Suppose H is a subgroup of a finite group of G. Then $|H| \mid |G|$.

2. **Corollary 12.5** Suppose G is a finte group and H is a proper subgroup. Then $|H| \leq |G|/2$.

3. **Lemma 12.7** Let $m, n \in \mathbb{N}$. Then $C_m \times C_n$ is cyclic iff $\gcd(m, n) = 1$.

4. **Theorem 12.8** For any positive integer t,

$$(\mathbb{Z}/p^t\mathbb{Z})^\times \cong C_{p^{t-1}(p-1)} \text{ if p is odd,}$$

$$(\mathbb{Z}/2^t\mathbb{Z})^\times \cong \begin{cases} 1 & if\ t = 1 \\ C_2 & if\ t = 2 \\ C_2 \times C_{2^{t-2}} & if\ t \geq 3 \end{cases}$$

5. **Corollary 12.10** Let $m \in \mathbb{N}$. Then $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic iff $m = 2, 4, p^t, 2p^t$. for some odd prime p and positive integer t. In particular, if m is an odd composite integer, then $(\mathbb{Z}/m\mathbb{Z})^\times$ is not cyclic.

6. **HW10 Q1** G is cyclic with order m iff for any $d \mid m$, there is a unique subgroup of G of order d. There are also $\phi(d)$ elements of G, assuming it is cyclic, of order d.

Probablistic Primality Testing

1. **Lemma 13.1** If $a^{n-1} \equiv \pmod{n}$ for every $a = 1 \cdots n-1$, then n is prime (Because it implies it is co-prime to every number before for it)
2. **Lemma 13.2** Let $F_n = \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{n-1} = 1\}$. It is a subgroup. (Side Note: if $F_n = (\mathbb{Z}/n\mathbb{Z})^\times$ then n is Carmichael and there exists infinitely many of them)
3. **HW10 3(b)** Let n be an odd int wit prime factorization $n = p_1^{k_1} + \cdots + p_r^{k_r}$ where $p_1, \cdots, p_r$ are odd primes. n is Carmichael iff $p_i^{k_i-1}(p_i - 1)$ divides $n-1$ for every $i = 1, \cdots, r$.
4. **Props 13.4** Carmichael Numbers are squarefree. (divisible by no-square integer aside from 1)
5. Carmichael Numbers n exhibit the property where for all $a \in \mathbb{Z}/n\mathbb{Z}$, we get that $a^n \equiv a \pmod{n}$.

Deterministic Primality Testing

1. **Exercise 14.1** Suppose $p \equiv 3 \pmod 4$ is a Sophie Germain prime. We get that $2p+1 \mid M_p$ and so M_p is not prime for $p > 3$.
2. **Exercise 14.2** Suppose p, q are primes such that $q \mid M_p$. We get that $q \equiv 1 \pmod{2p}$

The Gaussian and Eisentein integers

Actually fuck it, go to page 101 of package 4 instead for references in this section.

1. **Theorem 15.1** If p is a prime congruent to 1 *mod* 4, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$

   Theorem 15.2 If p is a prime congruent to 1 *mod* 3, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.