Useful Facts MATH 145. ExamPrep Summary

$\gcd(a^m-1, a^n-1) = a^{\gcd(m,n)}-1 \Rightarrow$ if $d \mid n$, then $x^d-1 \mid x^n-1$.

$\pi(x) \geq C \cdot \log x, \quad \forall x \geq 2$

$n = n_0 + n_1 p + \cdots + n_k p^k$, $s_p(n) = n_0 + n_1 + \cdots + n_k \Rightarrow v_p(n!) = \dfrac{n - s_p(n)}{p-1}$

$\forall m \geq 7$, $L_m \geq 2^m$ and $L_m \sim e^m$.

$$\mu(n) = \begin{cases} (-1)^{d(n)}, & n \text{ is square free} \\ 0 & \end{cases}$$

(where $d(n) = \#$ of distinct prime divisors)

also $\displaystyle\sum_{d \mid n} \mu(d) = \begin{cases} 1, & n=1 \\ 0, & n>1 \end{cases}$

Möbius Inversion: $f(n) = \displaystyle\sum_{d \mid n} g(d) \Rightarrow g(n) = \mu(d) \cdot f\left(\frac{n}{d}\right)$

- Ring Axioms, $\mathrm{char}(R) \mid |R|$.
- Ideal of Euclidean Domain generated by 1 element
- If $f(x) \in \mathbb{F}_p[x]$ irreducible, $\alpha = x + (f(x))$ in $\mathbb{F}_p[x]/(f(x))$
  then $f(x) = \displaystyle\prod_{i=0}^{n-1} (x - \alpha^{p^i})$
- In field of size q, q odd $\Rightarrow \frac{q+1}{2}$ squares; q even $\Rightarrow$ all elements are squares.
- $x^p - x + a \in \mathbb{F}_p[x]$ is irreducible.

- Splitting Field: smallest subfield of E containing $F[\alpha_1, \alpha_2, \dots, \alpha_n]$ where α_i are roots of $f(x)$.
- If E is a splitting field of $f(x)$ and $g(x)$ irreducible, $g(x)$ having 1 root in $E \Rightarrow g(x)$ splits completely in E.
- $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n - \zeta_n^{-1})$
- $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong C_{p^{k-1}(p-1)}$ cyclic
- $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic for $m = 2, 4, p^k, 2p^k$. p = odd prime $k \in \mathbb{N}$.
- $\pi_p(\Phi_m(x))$ factors as $\frac{\phi(m)}{O_m(p)}$ irreducibles in $\mathbb{F}_p[x]$.
- If $f(x) = g(x) \cdot h(x)$, $\Delta(f) = \Delta(g) \cdot \Delta(h) \cdot D^2$ for some $D \in \mathbb{F}_p^\times$.
- Carmichael, is a number m st: $a^{m-1} \equiv 1 \pmod{m}$, $\forall m \in (\mathbb{Z}/m\mathbb{Z})^\times$
- Finite integral Domain $\rightarrow$ field.
- $I \subseteq J$ ideals of R, S subring of R.

  then:
  - $R[x]/I[x] \cong (R/I)[x]$
  - ideals of R/I are of the form J/I.
  - $(S+I)/I \cong S/(S \cap I)$ 2^{nd} Iso
  - $(R/I)/(J/I) \cong R/J$ 3^{rd} Iso

$\mathbb{F}_{p^n}$ has a unique subring $\cong \mathbb{F}_{p^d}$ iff $d \mid n$.

Eisenstein: let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$

p prime, $p \mid a_i$, $\forall i = 0, \dots, n-1$, $p \nmid a_n$. $p^2 \nmid a_0$

Then f is irred. in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

$(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$

$\exists\, x, y \in \mathbb{Z}$ st $\gcd(a,b) = ax + by$

$\gcd(a,b) = \gcd(a, b - aq)$

$\nu_p(nm) = \nu_p(n) + \nu_p(m)$, $\quad \nu_p(n+m) \geq \min\{\nu_p(n), \nu_p(m)\}$

$L_n = \mathrm{lcm}(1, 2, \dots, n)$, $\quad \nu_p(L_n) = \left\lfloor \frac{\log n}{\log p} \right\rfloor$

$L_n \leq 4^{n-1} \Longrightarrow \prod_{p \leq n} p \leq 4^{n-1}$

$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$, $\quad \binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$

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

$m < n$, $m_a = m \,\%\, a$, $n_a = n \,\%\, a$, $\left\lfloor \frac{n}{a} \right\rfloor - \left\lfloor \frac{m}{a} \right\rfloor - \left\lfloor \frac{n-m}{a} \right\rfloor = \begin{cases} 1 & n_a < m_a \\ 0 & n_a \geq m_a \end{cases}$

$\nu_p\left(\binom{n}{m}\right) = \sum_{j=1}^{k} \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{m}{p^j} \right\rfloor - \left\lfloor \frac{n-m}{p^j} \right\rfloor \right)$

$\nu_p\left(\binom{2n}{n}\right) = 0$ if $\frac{2n}{3} < p \leq n$.

Bertrand's Postulate.

Dirichlet's Theorem.

$\Phi_q(x) = \frac{x^q - 1}{x - 1}$, q prime. if $p \mid \Phi_q(a)$ then $p \equiv 1 \pmod q$ or $p = q$.

$x^m - 1 = \prod_{k=1}^{m} (x - \zeta_m^k)$, $\Phi_m(x) = \prod_{\substack{1 \le k \le m \\ o(\zeta_m^k)}} (x - \zeta_m^k)$

$x^m - 1 = \prod_{d \mid m} \Phi_d(x)$, $m = \sum_{d \mid m} \phi(d)$

An Euclidean polynomial for $\equiv a \pmod m$ exists iff $a^2 \equiv 1 \pmod m$

$x \mapsto x + a$ bijects for $a \in R$

$x \mapsto xa$ bijects for $a \in R^\times$

First iso: $R/\ker f \cong \mathrm{im}(f)$

CRT: I, J ideals of R. If $I + J = R$, then:

$$R/(IJ) \cong R/I \times R/J.$$

$\phi(m) = m \cdot \prod_{p \mid m} \left(1 - \frac{1}{p}\right)$, $m = p_1^{k_1} \cdots p_r^{k_r}$

R ring, $|R| \cdot a = 0$, $a^{|R^\times|} = 1$ $\forall a \in R$.

Euler's Thm: $\gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod m$

PID: Every Ideal Generated by 1 element.

- In ring of char $R=p$, $(a+b)^{p^n}=a^{p^n}+b^{p^n}$, $\forall a,b\in R$ and $n\in\mathbb{N}$
- $\mathbb{F}_{p^d}\cong\mathbb{F}_p[x]/(g(x))$, for irreducible g of degree d.
  - F has a primitive element: $F^\times=\{\alpha,\alpha^2,\dots,\alpha^{p^n-1}\}$
- $x^{p^n}-x$ is the product of all monic irreducibles in $\mathbb{F}_p[x]$ of degree dividing n.
- Every polynomial in $\mathbb{F}_p[x]$ of degree $d|n$ splits completely in $\mathbb{F}_{p^n}[x]$
- $\mathbb{F}_{p^n}$ has a unique subring $\cong\mathbb{F}_{p^d}$ iff $d|n$
- $q=|F|$, $x^q-x=\prod_{\alpha\in F}(x-\alpha)$
- $\alpha_n=\alpha_{n-1}-\left[\dfrac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}\right]_p$ for Hensel lifting
- If $x^2\equiv a \pmod q$ has a solution $\forall$ prime q, then a is a perfect square.
- $C_m\cong\mathbb{Z}/m\mathbb{Z}$ under addition
- $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})\cong C_n$, generated by Frobenius map $\tau(x)=x^p$.
- C_n has subgroup of order $d|n$.
- $\mathrm{Aut}_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^n})\cong\langle\tau^d\rangle$
- $\mathbb{Z}/p^n\mathbb{Z}\not\cong\mathbb{F}_{p^n}$
- Field homomorphism is injective

- Algebraic integers: $F(\alpha) \cong F[\alpha] \cong F[x]/(f(x))$
    - minimal poly. of α, monic, irreducible.
- $\mathrm{Aut}_F(F(\alpha)) \xleftrightarrow[\text{biject}]{}$ distinct roots of $f(x)$ in $F(\alpha)$
  - $f(x)$ min poly of α, then $[F(\alpha):F] = \deg(f)$
  - $[\mathbb{Q}(\zeta_m):\mathbb{Q}] = \phi(m)$, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_m)) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$
- Gauss: $a(x)$, $b(x)$ have content $1 \Rightarrow a(x) \cdot b(x)$ have content 1.
- If $k(x) \in \mathbb{Z}[x]$, and $h, j \in \mathbb{Q}[x]$ are monic st: $k(x) = h(x) \cdot j(x)$

  then $h(x), j(x) \in \mathbb{Q}[x]$
- If f is symmetric, $\exists\, g(s_1, \dots, s_n) = f(x_1, \dots, x_n)$

  elementary symmetric polynomials.
- Discriminant: $\Delta(f) = \prod_{1 \le i < j \le n} (x_i - x_j)^2$

  roots.
- Sum of square's theorem.
- Lagrange's thm: order of subgroup divides order of group.