Midterm Q&A

1) Use extended euclidean algorithm to find $g^{-1} \in \mathbb{Z}_p^*$.

If $\gcd(g, p) = 1$ then $\exists$ u, v integers

$$ug + pv = 1$$

$$ug \equiv 1 \bmod p$$

$$u = g^{-1}$$

2)

2.12. Let G be a abelian group, let $d \geq 1$ be an integer, and define a subset of G by

$$G[d] = \{g \in G : g^d = e\}.$$

(a) Prove that if g is in $G[d]$, then g^{-1} is in $G[d]$.
(b) Suppose that G is commutative. Prove that if g_1 and g_2 are in $G[d]$, then their product $g_1 \star g_2$ is in $G[d]$.
(c) Deduce that if G is commutative, then $G[d]$ is a group.

Goal: Show that $G[d] \subset G$ is also a group.

We call $G[d]$ is a subgroup.

(i) Identity: e is an identity of $G[d]$ because $e^d = e$, hence $e \in G[d]$.

(ii) If $g \in G[d]$, then $g^{-1} \in G[d]$ because

$$g \cdot g^{-1} = e$$
$$(g \cdot g^{-1})^d = e$$
$$g^d \cdot (g^{-1})^d = e$$
$$(g^{-1})^d = e$$

(iii) closure. For all $g, h \in G[d]$, $g \cdot h \in G[d]$. because

$$(g.h)^d = g^d . h^d = e$$

(iv) associativity: $G[d] \subseteq G$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3) a) What's the order of 2 in $\mathbb{Z}_3^*$?

b) Whats the order of 4 in $\mathbb{Z}_5^*$?

c) Let p be prime.
What is the order of $p-1$ in $\mathbb{Z}_p^*$?
Justify your answer

---

a) $2, \quad 2^2 = 1$

$ord(2) = 2$

b) $4, \quad 4^2 = 1$

$ord(4) = 2$

c) $ord(p-1) = 2$

because $(p-1)^2 = p^2 - 2p + 1$

$\equiv 1 \mod p$

3. Solve

$$7^x \equiv 11 \mod 67$$

$ord(7)$ is a divisor of $66 = 2 \cdot 3 \cdot 11$

$ord(7) = 2 \cdot 3 \cdot 11 = P_1 P_2 P_3$

$n_1 = 3 \cdot 11 \quad g_1 = g^{n_1} \quad h_1 = h^{n_1} \quad ord(g_1) = 2$

$n_2 = 2 \cdot 11 \quad g_2 = g^{n_2} \quad h_2 = h^{n_2} \quad ord(g_2) = 3$

$n_3 = 2 \cdot 3 \quad g_3 = g^{n_3} \quad h_3 = h^{n_3} \quad ord(g_3) = 11$

Solve x_1, x_2, x_3

$$g_1^{x_1} = h_1, \quad g_2^{x_2} = h_2, \quad g_3^{x_3} = h_3$$

Solve x s.t. $x \equiv x_1 \mod P_1$
$x \equiv x_2 \mod P_2$ using CRT.
$x \equiv x_3 \mod P_3$

4.

Two congruences

$$\boxed{\begin{aligned} x &\equiv x_1 \bmod p_1 \\ x &\equiv x_2 \bmod p_2 \end{aligned}}$$

$$p_1 u + p_2 v = 1$$

$$x = x_1 p_2 v + x_2 p_1 u$$

Three congruences

$$\boxed{\begin{aligned} x &\equiv x_1 \bmod p_1 \\ x &\equiv x_2 \bmod p_2 \\ x &\equiv x_3 \bmod p_3 \end{aligned}}$$

$$n_1 = p_2 p_3$$

$$n_2 = p_1 p_3$$

$$n_3 = p_1 p_2$$

$$\gcd(n_i, p_i) = 1 \qquad n_i u_i + p_i v_i = 1$$

$$x = x_1 n_1 u_1 + x_2 n_2 u_2 + x_3 n_3 u_3$$

Abritary number of congruences

$$\boxed{x \equiv x_i \bmod p_i} \qquad N = p_1 \cdots p_n$$

$$n_i = N / p_i$$

Solve $n_i u_i + p_i v_i = 1$

$$x = \sum_{i=1}^{n} x_i n_i u_i$$

5) Prove that

$$(\mathbb{Z}_7^*, \cdot) \cong (\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +)$$

1	(0, 0)
2	(0, 1)
3	(0, 2)
4	(1, 0)
5	(1, 1)
6	(1, 2)

A generator of $\mathbb{Z}_7^* = 3$

A generator of $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) = (1, 1)$

order of an element divides order of group, which is $2 \cdot 3$

isomorphic function maps generator to generator

$$\begin{array}{ccc} 3 & 3^2 = 2 & 3^3 = 6 \\ \downarrow & \downarrow & \downarrow \\ (1,1) & (0,2) & (1,0) \end{array}$$

$f(3^i) = i(1,1)$