Name: ***Solutions***

No collaboration!	*One formula sheet is allowed.*
Cell phones out of sight.	*Answers must include supporting work.*
Basic calculators are allowed.	*Closed book and notes.*

(1) [10 pts] Suppose that G is an abelian group generated by x_1, x_2, x_3. Using a quantum algorithm we've learnt that x_1, x_2, x_3 are subject to the following relations:

$$r_1 = 6x_1 - 2x_2 + 6x_3 = 0$$
$$r_2 = -12x_1 + 6x_2 - 6x_3 = 0$$
$$r_3 = 12x_1 - 4x_2 + 42x_3 = 0.$$

Assuming that this set of relations is complete (all other relations follow from r_1, r_2, r_3), express G as a direct product of cyclic groups.

Solution: Compute the Smith normal form of the relation matrix

$$\begin{bmatrix} 6 & -2 & 6 \\ -12 & 6 & -6 \\ 12 & -4 & 42 \end{bmatrix} \to \begin{bmatrix} -2 & 6 & 6 \\ 6 & -12 & -6 \\ -4 & 12 & 42 \end{bmatrix} \to \begin{bmatrix} 2 & -6 & -6 \\ 6 & -12 & -6 \\ -4 & 12 & 42 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 0 \\ 6 & 6 & 12 \\ -4 & 0 & 30 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 0 \\ 0 & 6 & 12 \\ 0 & 0 & 30 \end{bmatrix} \to \begin{bmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 30 \end{bmatrix}$$

Thus, the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$.

(2) [10 pts] Consider the set of polynomials $R = \mathbb{Z}_{15}[x]$ with coefficient from $\mathbb{Z}_{15}$.

(a) Is x a zero divisor in R? Explain.

(b) Does 6 have a multiplicative inverse in R? Explain.

(c) Is R a ring? Explain.

(d) Is R a field? Explain.

(d) Consider the set $G = \{5^x \mid x \in \mathbb{N}\}$ of all powers of 5 in $\mathbb{Z}_{15}[x]$. Is $(G, \cdot)$ a group?

Solution:

(a) No, x is not a zero divisor in R, because for every nontrivial polynomial $f(x) = a_n x^n + \ldots + a_0$ we have

$$x \cdot f(x) = a_n x^{n+1} + \ldots + a_0 x \neq 0.$$

(b) $f(x) = a_n x^n + \ldots + a_0$ is a multiplicative inverse of 6 if

$$6f(x) = 6a_n x^n + \ldots + 6a_0 = 1 \text{ in } \mathbb{Z}_{15}[x],$$

which implies $6a_0 \equiv_{15} 1$, which is impossible because $\gcd(6, 15) = 3 \nmid 1$.

(c) Yes, $\mathbb{Z}_{15}[x]$ is a ring because

(d) No, R is not a field. In particular because 6 is not a unit.

(d) No, $G = \{5, 10\}$ does not contain 1.

(3) [10 pts] Let $f(x) = 2x^2 + x + 1 \in \mathbb{Z}_3[x]$.

(a) [3 pts] Prove that $E = \mathbb{Z}_3[x]/\langle f(x)\rangle$ is a field.

(b) [1 pt] What is $\chi(E)$ and $|E|$?

(c) [3 pts] Is $-x$ (negative x) primitive in E?

(d) [3 pts] Find $(x+2)^{-1}$ in E. Explain!

Solution:

(a) $f(x) = 2x^2 + x + 1 \in \mathbb{Z}_3[x]$ is quadratic that has no zeros in $\mathbb{Z}_3$:

$$f(0) = 1 \not\equiv_3 0 \qquad f(1) = 4 \not\equiv_3 0 \qquad f(2) = 11 \not\equiv_3 0.$$

Hence, $f(x)$ is irreducible and E is a field.

(b) Obviously, $\chi(E) = 3$ and $|E| = 3^2 = 9$.

(c) The size of the multiplicative group E^* of E is $9 - 1 = 8$. So, to check if $-x$ is primitive it is sufficient to check that

$$(-x)^2 = x^2 = x + 1 \neq 1 \text{ and } (-x)^4 = (x+1)^2 = x^2 + 2x + 1 = 2 \neq 1.$$

Thus, $-x$ is primitive.

(d) Consider a general element $ax + b \in E$ with unknown $a, b \in \mathbb{Z}_3$. Then

$$\begin{aligned}(ax+b)(x+2) &= ax^2 + (2a+b)x + 2b\\ &= bx + (a+2b)\end{aligned}$$

which should be 1. Hence,

$$\begin{cases} b \equiv_3 0 \\ a + 2b \equiv_3 1 \end{cases}$$

which gives $b = 0, a = 1$. Thus, $(x+2)^{-1} = x$.

(4) [10 pts] Consider the field from the previous problem

$$E = \mathbb{Z}_3[x]/\langle f(x)\rangle, \text{ where } f(x) = 2x^2 + x + 1 \in \mathbb{Z}_3[x]$$

Compute the powers of $-x$ one-by-one to find $\log_{-x}(x)$.

Solution: We've seen in the previous problem that $(-x)^4 = 2 = -1$. Hence, $\log_{-x}(x) = \log_{-x}(-x \cdot (-1)) = \log_{-x}(-x) + \log_{-x}(-1) = 1 + 4 = 5$.

(5) [10 pts] For polynomials $f(x) = 2x^4 + x^2 + 4x + 1$ and $g(x) = x^4 + x^3 + 2x + 2$ in $\mathbb{Z}_5[x]$.

(a) [5 pts] Compute $\gcd(f(x), g(x))$.

(b) [5 pts] Compute $\alpha(x), \beta(x) \in \mathbb{Z}_5[x]$ such that $\gcd(f(x), g(x)) = \alpha(x)f(x) + \beta(x)g(x)$.

Show ALL supporting work.

Solution: Using the Euclidean algorithm we obtain

$$\begin{aligned} f(x) &= 2g(x) + (3x^3 + x^2 + 2) & \Rightarrow \quad \gcd(f,g) &= \gcd(3x^3 + x^2 + 2, g) \\ g(x) &= (2x+3)(3x^3 + x^2 + 2) + (2x^2 + 3x + 1) & &= \gcd(3x^3 + x^2 + 2, 2x^2 + 3x + 1) \\ 3x^3 + x^2 + 2 &= (4x+2)(2x^2 + 3x + 1) + 0 & &= \gcd(0, 2x^2 + 3x + 1) = 2x^2 + 3x + 1. \end{aligned}$$

Since, the gcd must be monic, we multiply the result by 3 and get $\gcd(f, g) = x^2 + 4x + 3$.

Next, using the computations above

$$\begin{aligned} 2x^2 + 3x + 1 &= \mathbf{g(x)} - (2x+3)(\mathbf{3x^3 + x^2 + 2}) \\ &= \mathbf{g(x)} - (2x+3)(\mathbf{f(x)} - 2\mathbf{g(x)}) \\ &= \mathbf{g(x)}(1 + 2(2x+3)) - \mathbf{f(x)}(2x+3) \\ &= \mathbf{f(x)}(3x+2) + \mathbf{g(x)}(4x+2) \end{aligned}$$

Multiplying by 3 we get

$$\gcd(f, g) = x^2 + 4x + 3 = \mathbf{f(x)}(4x+1) + \mathbf{g(x)}(2x+1)$$

Thus, $\alpha(x) = 4x + 1$ and $\beta(x) = 2x + 1$.

(6) [10 pts] Consider an instance of Shamir's $(3,3)$-threshold scheme over $\mathbb{Z}_5$. The participants decide to compute the secret and reveal their shares

#1 $(3,2)$,
#2 $(1,1)$,
#3 $(4,1)$.

What is the secret?

Solution: If we know that $f(x) \in \mathbb{Z}_5[x]$ is cubic and $f(3)=2$, $f(1)=1$, $f(4)=1$, then

$$l_1(x) = \frac{x-x_2}{x_1-x_2}\frac{x-x_3}{x_1-x_3} = \frac{(x-1)(x-4)}{(3-1)(3-4)} = 2x^2+3.$$

$$l_2(x) = \frac{x-x_1}{x_2-x_1}\frac{x-x_3}{x_2-x_3} = \frac{(x-3)(x-4)}{(1-3)(1-4)} = x^2+3x+2.$$

$$l_3(x) = \frac{x-x_1}{x_3-x_1}\frac{x-x_2}{x_3-x_2} = \frac{(x-3)(x-1)}{(4-3)(4-1)} = 2x^2+2x+1.$$

Finally, combine Lagrange basis polynomials

$$2(2x^2+3)+(x^2+3x+2)+(2x^2+2x+1) = 2x^2+4.$$

Then $L(0)=4$.

(7) [10 pts] Consider the elliptic curve $\mathcal{E}$ defined by the equation $y^2 = x^3 + 2x + 2$ over $\mathbb{Z}_5$.

(a) [2pts] Is it singular?
(b) [2pts] Which of the points $(0,0), (0,4), (1,1), (3,2)$ belong to $\mathcal{E}$?
(c) [2pts] $(3,3) + (3,3) =$
(d) [2pts] $(1,3) + (3,3) =$
(e) [2pts] $-(1,3) =$

Solution:

	$\mathcal{O}$	$(1,0)$	$(2,2)$	$(2,3)$	$(3,0)$	$(4,2)$	$(4,3)$
$\mathcal{O}$	$\mathcal{O}$	$(1,0)$	$(2,2)$	$(2,3)$	$(3,0)$	$(4,2)$	$(4,3)$
$(1,0)$	$(1,0)$	$\mathcal{O}$	$(1,0)$	$(1,0)$	$(1,0)$	$(1,0)$	$(1,0)$
$(2,2)$	$(2,2)$	$(1,0)$	$(2,2)$	$\mathcal{O}$	$(4,2)$	$(4,3)$	$(3,0)$
$(2,3)$	$(2,3)$	$(1,0)$	$\mathcal{O}$	$(2,2)$	$(4,3)$	$(3,0)$	$(4,2)$
$(3,0)$	$(3,0)$	$(1,0)$	$(4,2)$	$(4,3)$	$\mathcal{O}$	$(2,2)$	$(2,3)$
$(4,2)$	$(4,2)$	$(1,0)$	$(4,3)$	$(3,0)$	$(2,2)$	$(2,3)$	$\mathcal{O}$
$(4,3)$	$(4,3)$	$(1,0)$	$(3,0)$	$(4,2)$	$(2,3)$	$\mathcal{O}$	$(2,2)$

(a) We have $a = 2$ and $b = 2$, so $4a^3 + 27b^2 = 4 \cdot 2^3 + 27 \cdot 2^2 = 140 \equiv_5 0$. Thus $\mathcal{E}$ is singular.
(b) By simply plugging in the given points to the equation for $\mathcal{E}$, we can see that none of the given points belong to $\mathcal{E}$.
(c) This is a typo. The point $(3,3)$ is not on $\mathcal{E}$. However, if it were, we could find $\lambda = 4$, $x_3 = 0$, and $y_3 = 4$. Thus we have $(3,3) + (3,3) = (0,4)$.
(d) This is also a typo. Neither of the given points are on $\mathcal{E}$. However, if they were, we could find $\lambda = 0$, $x_3 = 1$, $y_3 = 2$. Thus we have $(1,3) + (3,3) = (1,2)$.
(e) This is also a typo. The given point is not on $\mathcal{E}$. If it were, however, we could easily find $-(1,3) = (1,-3)$.

(8) [10 pts] Consider the elliptic curve $\mathcal{E}$ defined by the equation $y^2 = x^3 + 2x + 5$ over $\mathbb{Z}_{13}$. Its addition table is shown below

	$\mathcal{O}$	$(2,2)$	$(2,11)$	$(3,5)$	$(3,8)$	$(4,5)$	$(4,8)$	$(5,6)$	$(5,7)$	$(6,5)$	$(6,8)$	$(8,0)$
$\mathcal{O}$	$\mathcal{O}$	$(2,2)$	$(2,11)$	$(3,5)$	$(3,8)$	$(4,5)$	$(4,8)$	$(5,6)$	$(5,7)$	$(6,5)$	$(6,8)$	$(8,0)$
$(2,2)$	$(2,2)$	$(5,7)$	$\mathcal{O}$	$(4,5)$	$(5,6)$	$(6,5)$	$(3,8)$	$(2,11)$	$(3,5)$	$(8,0)$	$(4,8)$	$(6,8)$
$(2,11)$	$(2,11)$	$\mathcal{O}$	$(5,6)$	$(5,7)$	$(4,8)$	$(3,5)$	$(6,8)$	$(3,8)$	$(2,2)$	$(4,5)$	$(8,0)$	$(6,5)$
$(3,5)$	$(3,5)$	$(4,5)$	$(5,7)$	$(8,0)$	$\mathcal{O}$	$(6,8)$	$(2,11)$	$(2,2)$	$(6,5)$	$(4,8)$	$(5,6)$	$(3,8)$
$(3,8)$	$(3,8)$	$(5,6)$	$(4,8)$	$\mathcal{O}$	$(8,0)$	$(2,2)$	$(6,5)$	$(6,8)$	$(2,11)$	$(5,7)$	$(4,5)$	$(3,5)$
$(4,5)$	$(4,5)$	$(6,5)$	$(3,5)$	$(6,8)$	$(2,2)$	$(4,8)$	$\mathcal{O}$	$(5,7)$	$(8,0)$	$(3,8)$	$(2,11)$	$(5,6)$
$(4,8)$	$(4,8)$	$(3,8)$	$(6,8)$	$(2,11)$	$(6,5)$	$\mathcal{O}$	$(4,5)$	$(8,0)$	$(5,6)$	$(2,2)$	$(3,5)$	$(5,7)$
$(5,6)$	$(5,6)$	$(2,11)$	$(3,8)$	$(2,2)$	$(6,8)$	$(5,7)$	$(8,0)$	$(4,8)$	$\mathcal{O}$	$(3,5)$	$(6,5)$	$(4,5)$
$(5,7)$	$(5,7)$	$(3,5)$	$(2,2)$	$(6,5)$	$(2,11)$	$(8,0)$	$(5,6)$	$\mathcal{O}$	$(4,5)$	$(6,8)$	$(3,8)$	$(4,8)$
$(6,5)$	$(6,5)$	$(8,0)$	$(4,5)$	$(4,8)$	$(5,7)$	$(3,8)$	$(2,2)$	$(3,5)$	$(6,8)$	$(5,6)$	$\mathcal{O}$	$(2,11)$
$(6,8)$	$(6,8)$	$(4,8)$	$(8,0)$	$(5,6)$	$(4,5)$	$(2,11)$	$(3,5)$	$(6,5)$	$(3,8)$	$\mathcal{O}$	$(5,7)$	$(2,2)$
$(8,0)$	$(8,0)$	$(6,8)$	$(6,5)$	$(3,8)$	$(3,5)$	$(5,6)$	$(5,7)$	$(4,5)$	$(4,8)$	$(2,11)$	$(2,2)$	$\mathcal{O}$

(a) [2pt] Find the order of $(2,2)$.

(b) [4pts] If $\mathcal{E}$ is cyclic, then find ALL primitive points on $\mathcal{E}$. If $\mathcal{E}$ is not cyclic, then show that $\mathcal{E}$ has no primitive points.

(c) [4pts] Solve an instance $((2,2),(3,5),(6,5))$ of an ECCDH.

Solution:

(a) We can find multiples of $(2,2)$ using the given table:

$$\begin{array}{ccc} 1\cdot(2,2)=(2,2) & 2\cdot(2,2)=(5,7) & 3\cdot(2,2)=(3,5) \\ 4\cdot(2,2)=(4,5) & 5\cdot(2,2)=(6,5) & 6\cdot(2,2)=(8,0) \\ 7\cdot(2,2)=(6,8) & 8\cdot(2,2)=(4,8) & 9\cdot(2,2)=(3,8) \\ 10\cdot(2,2)=(5,6) & 11\cdot(2,2)=(2,11) & 12\cdot(2,2)=\mathcal{O} \end{array}$$

Hence, $|(2,2)| = 12$.

(b) We know that $\mathcal{E}$ is cyclic from (a), since $(2,2)$ generates $\mathcal{E}$. Looking at the table, we can see that all of the primitive points on $\mathcal{E}$ are as follows: $(2,2),(2,11),(6,5),(6,8)$.

(c) We are given $g=(2,2)$, $a\cdot g=(3,5)$, and $b\cdot g=(6,5)$. Using the table, we can then see that $a=(5,7)$ (since $(5,7)\cdot(2,2)=(3,5)$), and $b=(4,5)$ (since $(4,5)\cdot(2,2)=(6,5)$. Then we compute

$$(a\cdot b)\cdot g = ((5,7)\cdot(4,5))\cdot(2,2) = (8,0)\cdot(2,2) = (6,8).$$