Chapter 08

Mingjia Huo

Problem 8.1. By the definition of group, we have $\mathbb{G}$ has a identity and every element in $\mathbb{G}$ has a inverse.

Unique identity:
Given two identities $a, b \in \mathbb{G}$, we have $ab = a$ and $ab = b$. So $a = b$, and there is only one identity.

Unique inverse:
For element $a \in \mathbb{G}$, given it's inverse b, c, we have $ba = ab = e, ca = ac = e$. So $b = be = b(ac) = (ba)c = ec = c$, thus there is only one inverse of a.

Problem 8.3. $\mathbb{G}$ is finite:

- Closure: Since $g \in \mathbb{G}$, with the closure property, $\forall i \in \mathbb{N}, g^i \in \mathbb{G}$. So we have $\langle g \rangle \subseteq \mathbb{G}$, a close-set.
- Existence of an identity: $g^0 = e$. $\forall a \in \langle g \rangle$, we have $a \in \mathbb{G}$. So $ae = ea = a$.
- Existence of inverses: Since $\langle g \rangle \subseteq \mathbb{G}$, $\exists i, j \in \mathbb{N}, i < j, g^i = g^j$. There is a inverse of g^i in $\mathbb{G}$, denoted as a. So $e = ag^i = ag^j = ag^i g^{j-i} = g^{j-i}$. Let $t = j - i$. Thus $\forall s \in \mathbb{N}, s = kt + r, 0 \le r < t$, so $g^s = g^r$.
  - If $r = 0$, it's inverse is e.
  - If $r > 0$, it's inverse is g^{t-r}.

  So we get the inverse of g^s.
- Associativity: $\forall a, b, c \in \langle g \rangle$, we have $a, b, c \in \mathbb{G}$, which has associativity. Thus $\langle g \rangle$ has associativity.

$\mathbb{G}$ is infinite: give a counterexample:
Give $g = 1, \mathbb{G} = (\mathcal{Z}, +)$. Then $\langle g \rangle = \{0, 1, 2 \cdots\}$. But $\{1, 2 \cdots\}$ don't have their inverses, a contradiction.

Problem 8.8. Define $\mathbb{G} \times \mathbb{H} = \{(g, h) \mid g \in \mathbb{G}, h \in \mathbb{H}\}$, and the operation is $(a, b)(c, d) = (ab, cd)$.

- Closure: $\forall (a, b), (c, d) \in \mathbb{G} \times \mathbb{H}$, we have (ac, bd) with $ac \in \mathbb{G}, bd \in \mathbb{H}$. Thus $(ac, bd) \in \mathbb{G} \times \mathbb{H}$.
- Existence of an identity: The identities of $\mathbb{G}, \mathbb{H}$ are e_g, e_h respectively, so $\forall (a, b) \in \mathbb{G} \times \mathbb{H}$, $(a, b)(e_g, e_h) = (ae_g, be_h) = (a, b)$. And it's similar with $(e_g, e_h)(a, b)$. So the identity is (e_g, e_h).
- Existence of inverses: $\forall (a, b) \in \mathbb{G} \times \mathbb{H}$, denote $a^{-1} \in \mathbb{G}, b^{-1} \in \mathbb{H}$. So $(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e_g, e_h)$, which is the identity of $\mathbb{G} \times \mathbb{H}$. And it's similar with $(a^{-1}, b^{-1})(a, b)$. So the inverse is (a^{-1}, b^{-1}).
- Associativity: $((a_1, b_1)(a_2, b_2))(a_3, b_3) = ((a_1 a_2)a_3, (b_1 b_2)b_3) = (a_1(a_2 a_3), b_1(b_2 b_3)) = (a_1, b_1)((a_2, b_2)(a_3, b_3))$. The second equality holds for the associativity of $\mathbb{G}, \mathbb{H}$.

Problem 8.14. Construct $\mathcal{A}'$ as followed:

1. $\mathcal{A}'$ is given y. Set $cnt = 1$.
2. Uniformly choose $r \in \mathcal{Z}_N^*$. It's easy compute r^{-1} in $\log N$ time by Euclidean algorithm.
3. Compute $yr^e = y' \mod N$, and give y' to $\mathcal{A}$.
4. When $\mathcal{A}$ outputs x', check if $x'^e = y'$.
   - If so, output $x = x' r^{-1}$.
   - If not, then check the number of cnt. If $cnt < 500$, increase cnt by 1 and jump to step 2; else return a uniform $x \in \mathcal{Z}_N^*$.

In the above algorithm, $\mathcal{A}'$ can uniformly choose at most 99 r. Since r is uniform, then xr is uniform in $\mathcal{Z}_N^*$. Since

$$\Pr[\mathcal{A}([(xr)^e \mod N]) = xr] = 0.01,$$

we have $\Pr[\mathcal{A}([(xr)^e \mod N]) \neq xr] = 0.99$. Repeat 500 times, the probability of all failed is

$$\Pr[\mathcal{A}([(xr)^e \mod N]) \neq xr]^{500} \approx 0.006 < 0.01.$$

And

$$\Pr[\mathcal{A}'([(x)^e \mod N]) = x] = 1 - \Pr[\mathcal{A}([(xr)^e \mod N]) = xr]^{500} > 0.99.$$

Problem 8.16. Determine the points on the elliptic curve E : $y^2 = x^3 + 2x + 1$ over $\mathcal{Z}_{11}$. How many points are on this curve?

Firstly, the quadratic residues of 11 are $1, 4, 9, 5, 3$.

Define $f(x) = x^3 + 2x + 1$,

- $f(0) = 1$. So $(0, 1), (0, -1)$ is on the curve.
- $f(1) = 4$. So $(1, 2), (1, -2)$ is on the curve.
- $f(2) = 2$, a quadratic non-residue modulo 11.
- $f(3) = 1$. So $(3, 1), (3, -1)$ is on the curve.
- $f(4) = 7$, a quadratic non-residue modulo 11.
- $f(5) = 4$. So $(5, 2), (5, -2)$ is on the curve.
- $f(6) = 9$. So $(9, 3), (9, -3)$ is on the curve.
- $f(7) = 6$, a quadratic non-residue modulo 11.
- $f(8) = 1$. So $(8, 1), (8, -1)$ is on the curve.
- $f(9) = 0$. So $(9, 0)$ is on the curve.
- $f(10) = 9$. So $(10, 3), (10, -3)$ is on the curve.

Along with $\{\mathcal{O}\}$, there are totally 16 points on $y^2 = x^3 + 2x + 1$ over $\mathcal{Z}_{11}$.