Modular Exponentiation

(a). 8

(b). 160 = 32 + 128, 16

(c). $218^3 = (200 + 10 + 8)^3 = 8 \mod 9$

(d). $998^1 56 = (998^1 2)^1 3 = 1 \mod 13$

Sparsity of Primes

Provement equals to find a x that x+1, x+2, ... x+k are all not powers of primes. If a number can be divided by two distinct prime, then this number is not a prime power. This property can also apply to x+1, ... x+k these k integers. So we can select 2k distinct primes p1, p2, ... p2k-1, p2k and enforce the following constraints:

$$
\begin{aligned}
x + 1 &\equiv 0 \mod p_1 p_2 \\
x + 2 &\equiv 0 \mod p_3 p_4 \\
&\cdots \\
x + k &\equiv 0 \mod p_{2k-1} p_{2k}
\end{aligned}
$$

By Chinese Reminder Theorem, we can calculate the value of x so this x must exists, and thus x + 1 through x + k are all not prime powers.

LOTUS but for CRT

Since p and q are primes, so gcd(a, p) = 1 and gcd(a, q) = 1. By FLT,

$$a^{(p-1)(q-1)+1} = (a^{p-1})^{q-1} \cdot a \equiv 1^{q-1} \cdot a \equiv a \mod p$$

$$a^{(p-1)(q-1)+1} = (a^{q-1})^{p-1} \cdot a \equiv 1^{p-1} \cdot a \equiv a \mod q$$

Consider the system of congruences,

$$x \equiv a \mod p$$

$$x \equiv a \mod q$$

By CRT, we can calculate a value of x,

$$x = a \cdot q^{-1} (\mod p) \cdot q + a \cdot p^{-1} (\mod q) \cdot p (\mod pq)$$

$$x = a(\cdot q^{-1}(\mod p) \cdot q + p^{-1}(\mod q) \cdot p)(\mod pq)$$

Since p and q are co-prime, by Bezout's lemma,

$$g \cdot p + h \cdot q = 1$$

where g and h are respectively $p^{-1}(\mod q)$ and $q^{-1}(\mod p)$. Hence,

$$x = a(g \cdot p + h \cdot q) \equiv a \cdot 1 \mod pq$$

Therefore, let $x = a^{(p-1)(q-1)+1}$, $x \equiv a \mod p$ and $x \equiv a \mod q$, then $x \equiv a \mod pq$. We conclude that $a^{(p-1)(q-1)+1} \equiv a \mod pq$.

Squared RSA

(a). Prove the identity $a^{p(p-1)} \equiv 1 \mod p^2$ where a is coprime to p and p is a prime.

Let

$$S = \{1, 2, 3, \cdots p^2 - 1\}$$

where each element is coprime to p.

and

$$T = \{a, 2a, 3a, \cdots a \cdot p^2 - 1\}$$

Exclude $\{p^2 - p, p^2 - 2p, \cdots p^2 - (p-1)p\}$ from 1 to $p^2 - 1$, we know that $|S| = p^2 - 1 - (p-1) = p(p-1)$.

Let prove $S = T$:

- $S \subseteq T$: Since gcd(a, p) = 1, $a^{-1} \mod p^2$ exists, and also gcd(a^{-1}, p) = 1. Let $x \in S$, and gcd(x, p) = 1, so gcd($a^{-1}x$, p) = 1, so $a^{-1}x \in S$. $a(a^{-1}x) = x \in T$. Hence $S \subseteq T$.
- $T \subseteq T$: Let $ax \in T$ where $x \in S$, we know that gcd(x, p) = 1, gcd(a, p) = 1, and ax is also coprime to p as well. Since S include all distinct numbers from 1 to $p^2 - 1$ where each number is coprime to p. So $ax \in S$. We conclude.

Since S = T, we know that,

$$\prod_{s_i \in S} s_i = \prod_{t_i \in T} t_i \mod p^2$$

$$\prod_{t_i \in T} t_i = \prod_{s_i \in S} s_i \cdot a = a^{|S|} \cdot \prod_{s_i \in S} s_i = \prod_{s_i \in S} s_i \mod p^2$$

Since each $s_i \in S$ is coprime to p, $\prod_{s_i \in S} s_i$ is also coprime to p^2. Hence we can multiply both sides of our equivalence with the inverse of $\prod_{s_i \in S} s_i \mod p^2$ to obtain $a^{p(p-1)} \equiv 1 \mod p^2$. Thus we conclude.

(b). Prove $(x^e)^d \equiv x \mod p^2q^2$.
We know that $ed \equiv 1 \mod p(p-1)q(q-1)$, thus $ed = 1 + kpq(p-1)(q-1)$.
Our claim is that $x^{ed} - x \equiv 1 \mod pq(p-1)(q-1)$.

$x^{ed} - x = x(x^{kpq(p-1)(q-1)} - 1)$

Now we claim that the expression $x(x^{kpq(p-1)(q-1)} - 1)$ is divisible by p^2. To see this, we consider two case:

- *Case 1:* x is divisible by p^2, the expression is clearly divisible by p^2.
- *Case 2:* x is not divisible by p^2, by FLT and part a, the expression $\equiv x(1^{kq(q-1)} - 1) \equiv 0 \mod p^2$.

By an entirely symmetrical argument, the expression is also divisible by q^2. Since p and q is primes, the expression must be divisible by p^2q^2. Thus, we conclude.

Polynomials over Galois Fields

(a).

$$
\begin{aligned}
q(x) &= x^p - x \mod p \\
q(x) &= x(x^{p-1} - x) \mod p \\
q(x) &= 0 \mod p \\
q(x) &= \prod_{k=0}^{p-1} (x - k)
\end{aligned}
$$

(b). By Lagrange interpolation, passing through p points (0, f(0)), (1, f(0)), ... (p-1, f(p-1)) there is a unique polynomial of at most p-1 degree $\widetilde{f}(x)$.

Alternatively, by FLT, let d >= p, we know that,

$$
\begin{aligned}
x^d &= x^{d-(p-1)+(p-1)} \\
&\equiv x^{d-(p-1)} \mod p \\
&\equiv x^{d-2(p-1)} \mod p \\
&\dots
\end{aligned}
$$

So there must be a integer k to let $d - k(p-1) < p$, and $x^d \equiv x^{d-k(p-1)} \mod p$ by this k. We can apply this property to each x^n in f(x) where n >= p and obtain a polynomial with at most p-1 degree.

(c). Lemma: *The roots of R(x)=P(x)Q(x) are the union of the roots of P and Q*, the above claim clearly holds.
Let U be the union of the roots of P and Q, $\forall x \in \mathbb{R}$, there are two cases below:

- *$x \in U$:* Hence $P(x) = 0 \vee Q(x) = 0$, then $R(x) = 0$.
- *$x \notin U$:* Hence $P(x) \neq 0 \wedge Q(x) \neq 0$, then $R(x) \neq 0$.

Therefore, the lemma holds.

Suppose that P(x) and Q(x) are both non-zero polynomials and only have limited number of roots, hence R(x) also has limited roots. By contrapositive, since $x \in \mathbb{R}$, there must exists a x_{nozero} with which $P(x_{nozero}) \neq 0$ and $Q(x_{nozero}) \neq 0$, then $P(x_{nozero})Q(x_{nozero}) \neq 0$.

(d). In GF(p), $x^{p-1} - 1$ and x are both non zero polynomials, but their product $x^p - x \equiv 0 \mod p$ by FLT.

Packet Requirements

(a). Suppose Bob get n+2k-1 packets, where exists k corrupted packets.

If Bob select n uncorrupted packets, and get the interpolated polynomial f. Then f will pass through k-1 packets additionally.

If Bob select n packets consist of c corrupted packets and n-c uncorrupted packets. The remaining 2k-1 packets contains k-1+c uncorrupted packets and k-c corrupted. Note that the interpolated polynomial can pass through at most n-1 corrupted packets. So the polynomial can additionally pass through (n-1)-(n-c)=c-1 uncorrupted packets, and k-c corrupted packets, that is additional c-1 + k-c = k-1 packets, which is the same as the correct case above. Hence Bob cannot distinguish.

(b). Suppose Bob get n+2k packets, where exists k corrupted packets.

If Bob select n uncorrupted packets and get the corrected polynomial. Then polynomial will pass through k packets additionally.

If Bob select n packets consist of c corrupted packets and n-c uncorrupted packets. The remaining 2k packets contains k+c uncorrupted packets and k-c corrupted. Note that the interpolated polynomial can pass through at most n-1 corrupted packets. So the polynomial can additionally pass through (n-1)-(n-c)=c-1 uncorrupted packets, and k-c corrupted packets, that is additional c-1 + k-c = k-1 packets, which is different from k in the correct case. Hence Bob can distinguish.

ALice and Bob

(a). He can recover the origin message. $Q(x) = x^3 + 5x^2 + 5x + 4, E(x) = x3$. Hence the $P(x) = x^2 + x + 1$, the x-value of the packet Eve changed is 3.

(b). Since Bob know that there still remains 3 points uncorrupted and 2 points are corrupted. So the remaining 3 corrected points are always on the degree 1 polynomial that Alice encoded her message on. If Bob find multiple degree 1 polynomial across 3 points, then he will not be able to determine Alice's message, but if only one is found, he can.

In this case, if $x = 5, 6, 10$, Bob cannot do well.

(c). Alice can compile message 1 to 6 to a degree 5 polynomial and send 10 points about the polynomial to channel A. Then compile message 7 to 9 to a degree 2 polynomial and send 10 points about the polynomial to channel B. Bob can decode the degree 5 polynomial from 6 points from channel A and the degree 2 polynomial from 5 uncorrupted points and 1 corrupted point from channel B. For channel b, it can effectively pass a degree 3 polynomial with 5 uncorrupted points and one corrupted. So, there is even some redundancy.