CS70–Spring 2013 — Homework 5

Felix He, SID 303308****

April 9, 2024

Collaborators: None

1. Polynomials and modular arithmetic

1. True.

$$(a+b)^3 \equiv a^3 + 3a^2b + 3b^2a + b^3 \equiv a^3 + b^3 \; mod \; 3$$

since $3a^2b + 3b^2a$ is multiple of 3.

2. False.

$$(a+b)^3 \equiv a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

$6a^2b^2$ might not be multiple of 4, so not equal.

3. False.

$$(a+b)^4 \equiv a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \equiv a^5 + b^5 \; mod \; 5$$

$5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4$ is multiple of 5.

2. More polynomials!

1. Use strong induction.
Base case: $n = 0$, $P_0(7) \equiv 19 \; mod \; 19 \equiv 0 \; mod \; 19$, $n = 1$, $P_1(7) \equiv 19 \; mod \; 19 \equiv 0 \; mod \; 19$

IH: Assume $P_n(7) \equiv 0 \; mod \; 9$ holds true for $n \leq k$

IS: $n = k+1$, $P_{k+1}(7) = 7P_{k-1}(7) - P_k(7)$, $P_{k-1}(7)$ and $P_k(7)$ are $0 \; mod \; 19$,
so $P_{k+1}(7) \equiv 0 \; mod \; 19$

2. Similarly we can use strong induction to prove $P_n(x)$ is at most degree n, and we know q is prime, so it's working on a $GF(q)$ field. Then we can use property 1 to say $P_{2013}(x)$ has at most 2013 roots.

3. Solving systems of equations

1. 1. (mod 3)

$$
\begin{aligned}
x + y &= 2 \\
0 + y &= 2
\end{aligned}
$$

   2. (mod 5)

$$
\begin{aligned}
3x + 2y &= 2 \\
3x + 4y &= 3
\end{aligned}
$$

2. 1. (mod 3)

$$x = 0,\ y = 2 \text{ (mod 3)}$$

   2. (mod 5)

$$x = 2,\ y = 3 \text{ (mod 5)}$$

3. Use CRT, we can have

$$
\begin{aligned}
x &= 0 \times \frac{15}{3} \times (\frac{15}{3})^{-1} + 2 \times \frac{15}{5} \times (\frac{15}{5})^{-1} \\
&= 2 \times 3 \times 2 \\
&= 12 \quad \text{mod } 15 \\
y &= 2 \times \frac{15}{3} \times (\frac{15}{3})^{-1} + 3 \times \frac{15}{5} \times (\frac{15}{5})^{-1} \\
&= 2 \times 5 \times 2 + 3 \times 3 \times 2 \\
&= 8 \quad \text{mod } 15
\end{aligned}
$$

   And we know, if we put it back,

$$
\begin{aligned}
13x_{15} + 7y_{15} &= 2 \; mod \; 3 = 2 \; mod \; 5 \\
3x_{15} + 4y_{15} &= 2 \; mod \; 3 = 3 \; mod \; 5
\end{aligned}
$$

   And for the RHS of the linear equations, we know 3 and 5 are co-prime, so it also satisfy the CRT, the orignal 2 mod 15 is the unique integer that satisfies 2 mod 3 and 2 mod 5, 8 mod 15 satisfies 2 mod 3 and 3 mod 5.

4. You be the grader

F. The wrong part is taking square root. It's not valid in mod m.
For example.
$x = 2, y = 0, m = 16$, then

$$(x^2 - y^2)^2 \equiv 16 \text{(mod m)} \equiv 0 \text{(mod m)}$$

However,

$$(x^2 - y^2) \equiv 4 \text{(mod m)} \not\equiv 0 \text{(mod m)}$$

Similarly, we cannot take the square root in the final step.

5. Wait... We don’t need to play at the same time?

1. without a third party, it’s hard to confirm simultaneously, one person might see the choice of another. And they must play asynchronously.

2. 1. Alice and Bob both have their public key and private key. Alice sends Bob E(x1, A’s public key), then Bob receives and sends Alice E(x2, B’s public key). Neither of them can decrypt the message since they don’t have each other’s private key.
   2. Then both of them can reveal their choice x1’, x2’ to each other. Then they can compare whether E(x1’, A’s public key) = E(x1, A’s public key), E(x2’, B’s public key) = E(x2, B’s public key), if equal, it means x1 = x1’, x2 = x2’. If not it implies the other change his choice.
   3. Since there are only 3 options, which means E(x, public key) can only have 3 values, the other can calculate in advance to compare the value. So instead of sending the choice x, Alice and Bob can send ’x+random number’ such as ’x19960525’, as long as he or she remember that appended random number, and reveal it in step 2.