CIS 3362 11/6/24

(1) Walk through my code for adding + multiplying pt.

(2) Cyclic nature of the points

(3) Using elliptic curves for cryptography

Last Time

Defined a curve $E_p(a,b)$ $y^2 \equiv (x^3 + ax + b) \bmod p$

Defined Addition

- $P + P \rightarrow$ different formula λ (slope)
- $P + Q \rightarrow$ regular formula λ
- Imagine $\underbrace{P + P + P + P \cdots + P}_{k \text{ ~~value~~ pts } P} = \mathcal{O}$ (Additive identity)

add

Define multiplication $kP = \underbrace{P + P + \cdots + P}_{k \text{ times}}$

(k: Int, P: Point)

Code Addition $O(1)$ * Arithmetic Ops

Note GCD involve $O(\lg p)$ more accurate.

For Multiplication k could get pretty big

very large

```
mult ( Point P, int k ) {
    if (k == 0) return O
    if (k == 1) return P
    if (k % 2 == 0) {
        tmp = mult(P, k/2);
        return add(tmp, tmp);
    }
    tmp = mult(P, k-1)
    return add(tmp, P)
}
```

Divide + Conquer
Very simple
Fast
Modular
Expo

Runtime = O(log k * time(add))

↳ Quite manageable.

List

1. (3,10) = P
2. (7,12) = 2P
3. (19,5) = 3P
4. (17,3) = 4P
5. (9,16)
⋮
9. (0,1)
28. Origin = 28P

29. (3,10) = 29P

Let P = (3,10)
What is
85 × P

37P
↓
which entry

37P = 28P + 9P
= 9P

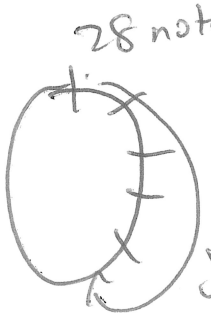
0 = 28P = 56P = 84P

85P = 84P + P
= O + P = (3,10)

Old list $P, 2P, 3P, 4P, \ldots \quad 28P = O$

new list $11P, 22P, 33P, 16P, 27P, 40P$, etc.

$\downarrow 5P \qquad \downarrow 12P$



Jump by 11 each time since $\gcd(11, 28) = 1$
I'll hit each notch once before returning where I started

list = $21P, 42P, 35P, \boxed{28P}$

$\downarrow 14P \qquad \downarrow 7P$

Jump by 21, then $\gcd(21, 28) = 7$, so my cycle size will be $\frac{28}{7} = 4$

If the cycle size for point P is n, then the cycle size for point kP is $\frac{n}{\gcd(k,n)}$.

Diffie-Hellman Key Exchange with Elliptic Curves

Public Components

1. $E_p(a,b)$ - specific elliptic curve
2. G - point with a large order
   [order = min value of k (positive) such that $kP = O$ (origin)]
   let n = order of G

Alice		Bob
Picks n_A (secret), $1 < n_A < n$		Picks n_B (secret) $1 < n_B < n$
Sends Bob	$T_1 = n_A \times G$ →	
	← $T_2 = n_B \times G$	Send this to Alice
Alice receives T_2 and calculates $n_A \times T_2$		Bob receives T_1 and calculates $n_B \times T_1$
$= (n_A \times n_B) \times G$		$= (n_B \times n_A) \times G$
↓ ↓ numbers pt	Given G, curve and given $T_1 = n_A G$ it's hard to figure out n_A	↑ ↑ number pt

In regular Diffie-Hellman knowing $g^a \bmod p$ and g and p doesn't help you to find a.