Elliptic-curve cryptography (**ECC**) is an approach to public-key cryptography based on the algebraic structure of elliptic curves points over finite fields.
ECC requires smaller keys compared to non-ECC cryptography to provide equivalent security.
For example, to achieve the same security ensured by ECC having private key of 256 bit length, it is required to use 3000 bit private key length for RSA cryptosystem and others.

Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks.
Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme.

Elliptic Curve Digital Signature Algorithm - Bitcoin Wiki **(ECDSA)**
https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm Feb 10, 2015
Elliptic Curve Digital Signature Algorithm or **ECDSA** is a cryptographic algorithm used by Bitcoin to ensure that funds can only be spent by their owner.
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

Finite Field denoted by F_p (or rarely Z_p), when: p is prime.
$F_p=\{0, 1, 2, 3, \ldots, p-1\}$; $+_{\text{mod } p}$, $-_{\text{mod } p}$, $\bullet_{\text{mod } p}$, $:_{\text{mod } p}$. $a, b, c \in F_p$: $a*(b+c) = a*b + a*c \mod p$
Cyclic Group: $Z_p^* = \{1, 2, 3, \ldots, p-1\}$; $\bullet_{\text{mod } p}$, $:_{\text{mod } p}$.
For example, if p=11, then one of the generetors is g=2. $Z_p^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

p=11
xa=∈

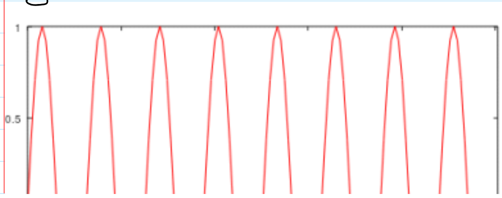
If g is a generator in Z_p^* then $Z_p^* = \{g^i \mod p \mid i = 0, 1, 2, \ldots, p-2\}$
If $p = 11$, then $g=2$ is a generator $Z_{11}^* = \{2^i \mod p \mid i = 0, 1, 2, \ldots, 9\}$

The main function used in cryptography was Discrete Exponent Function - DEF:
DEF(x) = g^x mod p = a.

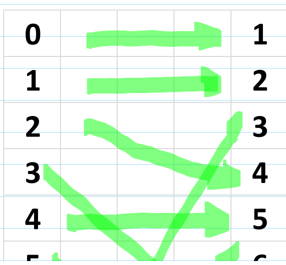
x	0	1	2	3	4	5	6	7	8	9	10
2^x **mod** p	1	2	4	8	5	10	9	7	3	6	1

Discrete Exponent Function - DEF(x)=g^x **mod** p
x is in $Z_{p-1} = Z_{10} = \{0, 1, 2, \ldots, 9\}$;
DEF(x) is in $Z_p^* = Z_{11}^* = \{1, 2, 3, \ldots, 10\}$;
DEF: $Z_{p-1} \rightarrow Z_p^*$.
Fermat theorem: if p is prime, then for any z: $z^{p-1}=1$ mod p.
If g is a generator in Z_p^* then DEF is 1-to-1 mapping.

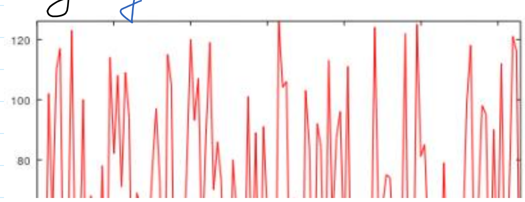
$y = \sin x$

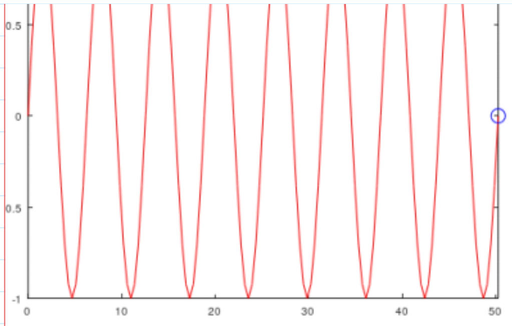


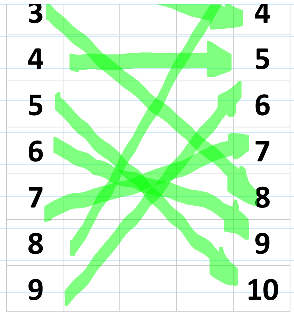
$x \in Z_{10}$ $a \in Z_{11}^*$

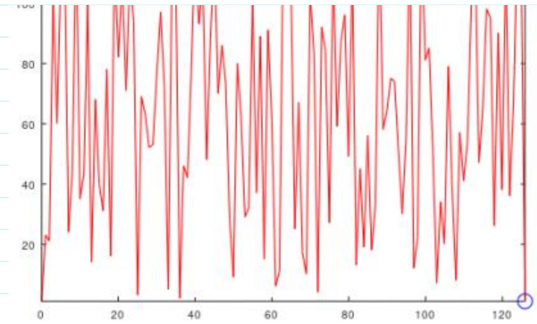


$p = 127$
$y = g^x \mod 127$









Multiplicative Group Z_p^*	Additive Group $Z_{p\text{-}1}^+$
$Z_p^*=\{1, 2, 3, \ldots, p\text{-}1\}$	$Z_{p\text{-}1}^+=\{0, 1, 2, 3, \ldots, p\text{-}2\}$
Operation: multiplication mod p	Operation: addition mod (p**-1**)
Neutral element is **1**.	Neutral element is **0**.
Generator g: $Z_p^*=\{ g^i;\ i=0,1,2, \ldots, p\text{-}1\}$ Two criterions to find g when p is strong prime. $g^n=1 \bmod p$ and $g^n\neq 1 \bmod p$ if $n<p$.	Generator g: $Z_{p\text{-}1}^+=\{i\bullet g;\ i=0,1, 2,\ldots,p\text{-}2\}$ E.g. $g=1$. $(p\text{-}1)\bullet g=0 \bmod (p\text{-}1)$ and $n\bullet g\neq 0 \bmod (p\text{-}1)$ if $n<p\text{-}2$.
Modular exponent: $t=g^k \bmod p$ $t= g\bullet g\bullet g\bullet \ldots\bullet g \bmod p$; k–times.	Modular multiplication: $t=k\bullet g \bmod p\text{-}1$ $t= g+g+g+ \ldots+g \bmod p\text{-}1$; k–times.

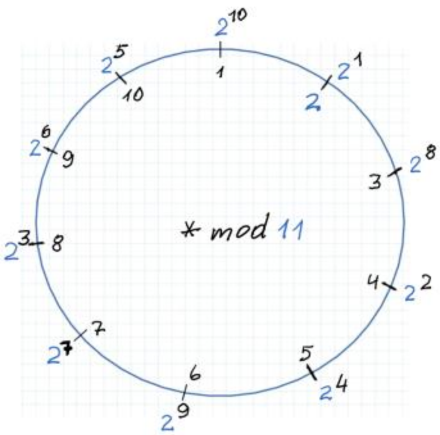
p = 11, p-1 = 10

$\bullet_{\text{mod } p}$

$Z_{11}^*=\{1, 2, \ldots, 10\}$

$|Z_{11}^*|=10$, g=2.

x		2^x
		mod 11
0	→	1
1	→	2
2	→	4
3	→	8
4	→	5
5	→	10
6	→	9
7	→	7
8	→	3
9	→	6
~~10~~	→	1



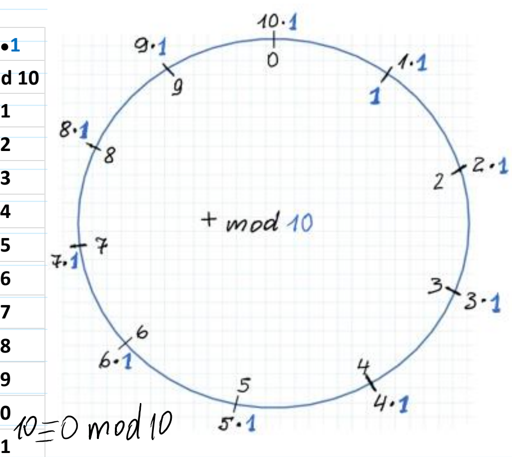
p = 11, p-1 = 10

$+_{\text{mod } (p\text{-}1)}$

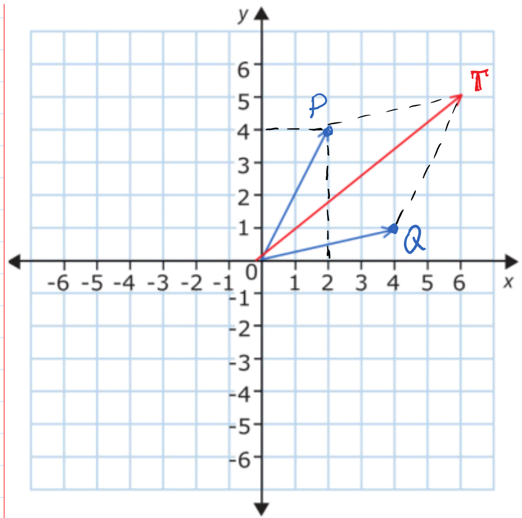
$Z_{10}^+=\{0, 1, 2, \ldots, 9\}$

$|Z_{10}^+|=10$; g=1.

x		x•1
		mod 10
0	→	1
1	→	2
2	→	3
3	→	4
4	→	5
5	→	6
6	→	7
7	→	8
8	→	9
9	→	0
10	→	1



Coordinate systems XOY in subsequent examples are defined in the plane of real numbers.

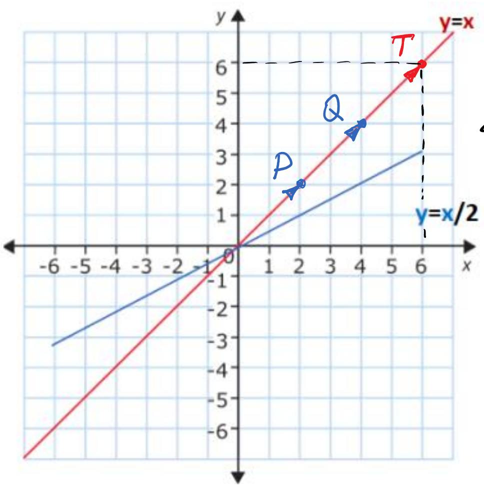


$$\left.\begin{aligned} P(x_P, y_P) &= (2,4) \\ Q(x_Q, y_Q) &= (4,1) \end{aligned}\right\} \begin{aligned} P+Q &= (2+4,\ 4+1) \\ T = P+Q &= (6,5) \end{aligned}$$

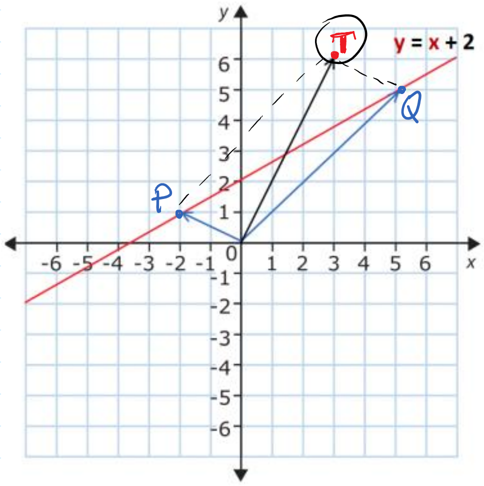
$$T = P(x_P, y_P) \overset{\boxplus}{+} Q(x_Q, y_Q) =$$
$$= T(x_P + x_Q,\ y_P + y_Q) = T(x_T, y_T)$$

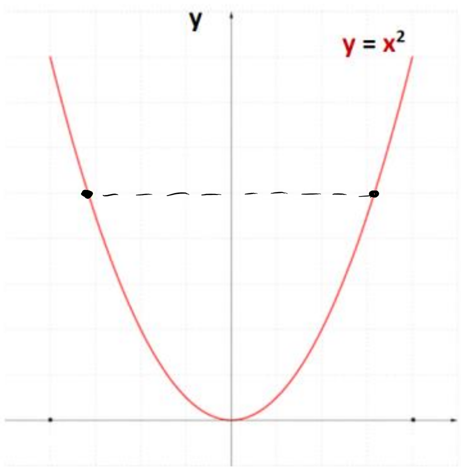
$$\left.\begin{aligned} x_T &= x_P + x_Q \\ y_T &= y_P + y_Q \end{aligned}\right\}$$

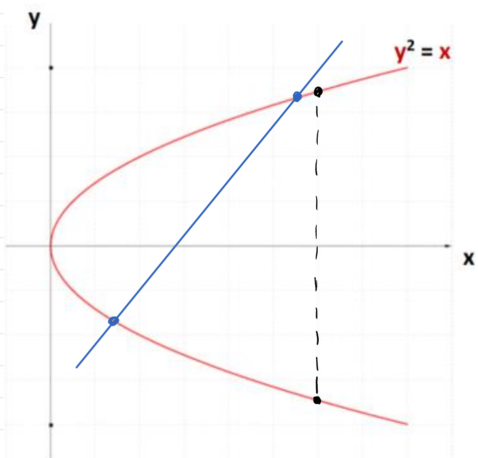
$$T_2 = P + P = 2P =$$

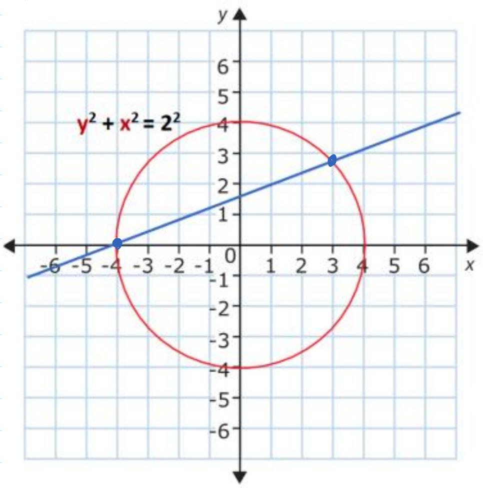


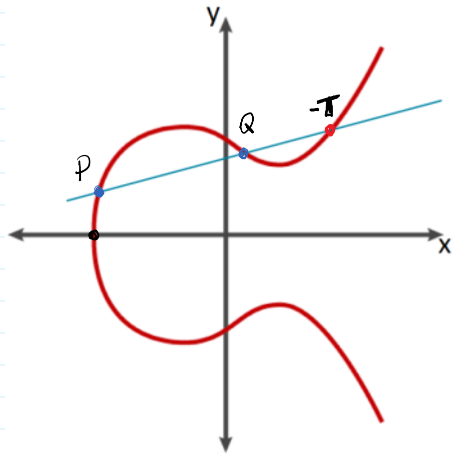
$$x_T = 2+4 = 6$$
$$y_T = 2+4 = 6$$
$$|T| =$$
$$= \sqrt{6^2 + 6^2}$$







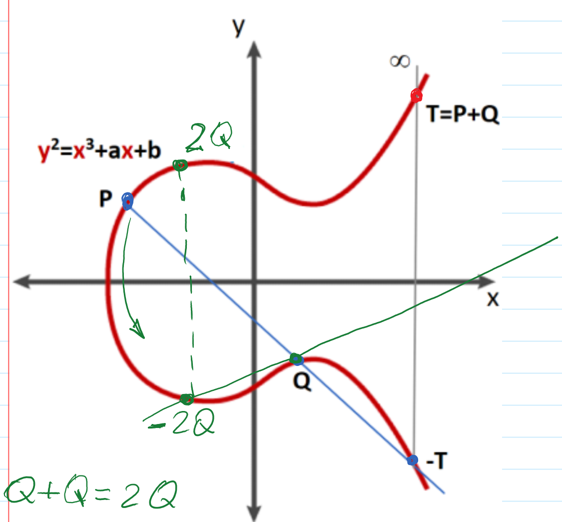




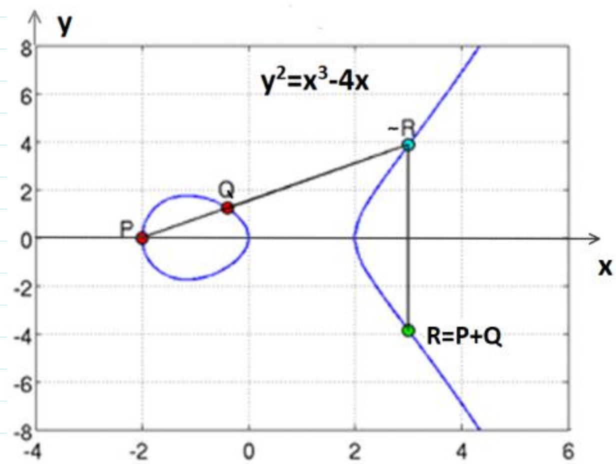
Elliptic curve ha a property that if line crosses two points, then there is a third crossing point in the curve.

Points in the plane or plane curve we denote by the capital letters, e.g. **A**, **G**, **P**, **Q**, etc.
Numbers-scalars we denote by the lowercase letters, e.g., **a**, **g**, **x**, **y**, **z**, etc.

Addition of points P and Q in EC: **P + Q = T**
$\mathbf{P(x_P,y_P) + Q(x_Q,y_Q) = T(x_T,y_T)}$



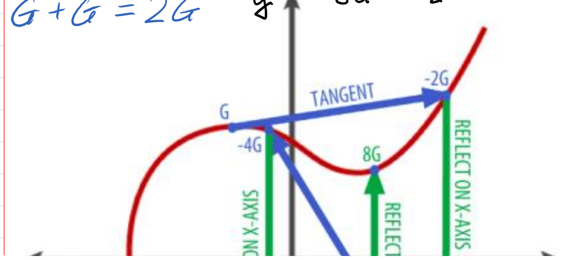
Q+Q=2Q

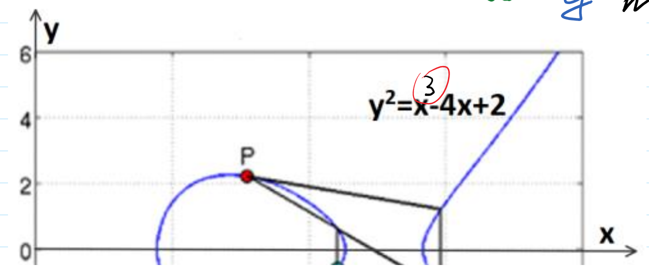


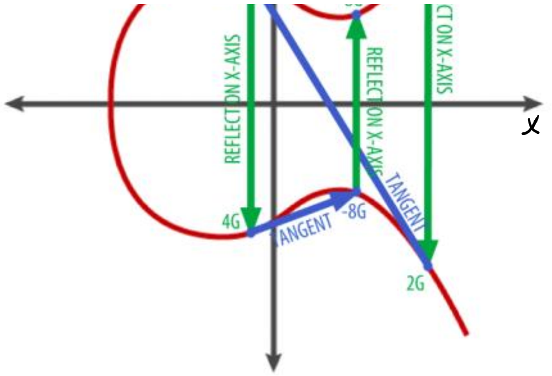
$5-5 \mod 10 = 0$ $\qquad T-T = „0" \longrightarrow T+(-T) = „0" \equiv \infty$
$7+0 \mod 10 = 7$ $\qquad T+\infty = T$

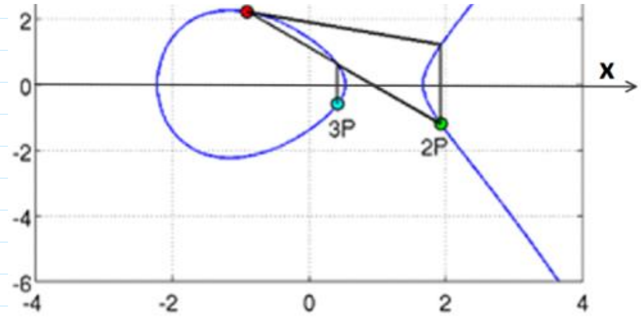
When z is large, $z \sim 2^{256} \longrightarrow |z| = 256$ bits:
Doubling of points allows effectively compute point $A = zG$
$a = g^x \mod p$

$G+G=2G$ $\qquad 8G = 2^3 G$









ECDSA animacija

[Signing and Verifying Ethereum Signatures – Yos Riady · Software Craftsman]

https://medium.com/coinmonks/elliptic-curve-cryptography-6de8fc748b8b

For current cryptographic purposes, an *elliptic curve* is a plane curve over a finite field F_p={0, 1, 2, 3, …, p-1}, (rather than the real numbers) p-is prime.
Which consists of the points satisfying the equation over F_p

$$y^2=x^3+ax+b \mod p$$

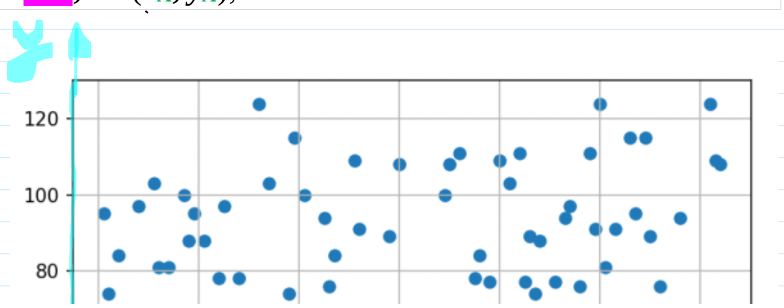
along with a distinguished point at infinity, denoted by ***0*** (∞).
Finite field is an algebraic structure, where 4 algebraic operations: $+_{\text{mod } p}$, $-_{\text{mod } p}$, $´_{\text{mod } p}$, $:_{\text{mod } p}$ are defined except the division by 0 excluded.

Elliptic Curve Group (ECG)
Number of points **N** of Elliptic Curve with coordinates (x, y) is an order of ECG.
Addition operation ⊞ of points in ECG: let points $P(x_P,y_P)$ and $Q(x_Q,y_Q)$ are in EC with coordinates (x_P,y_P) and (x_Q,y_Q) then P ⊞ Q = T with coordinates (x_T,y_T) in EC.
Neutral element is group zero ***0*** at the infinity (∞) of [XOY] plane.
Multiplication of any EC point G by scalar z: T=z∗G; T=G ⊞ G ⊞ G ⊞ ...⊞ G; z–times.
Generator–Base Point G: ECG={ i∗G; i=1,2,…,N}; N∗G=0 and q∗G≠0 if q<N.

ElGamal Cryptosystem (CS)	**Elliptic Curve Cryptosystem (CS)**
PP=(strongprime p, generator g); p=255996887; g=22;	**PP**=(EC **secp256k1**; BasePoint-Generator G; prime p; param. a, b); Parameters a, b defines EC equation $y^2=x^3+ax+b$ **mod** p over F_p.
PrK=x; >> **x**=randi(p-1).	**PrK** $_{\text{ECC}}$=**z**; >> **z**=randi(p-1).
PuK=a=g^x mod p.	**PuK**$_{\text{ECC}}$=A=**z**∗G.
Alice A: **x**=1975596; a=210649132;	**Alice** A: **z**=…..; A=(x_A, y_A);

p = 127

127 | 2
12   63,5
7
7
0



$\frac{x}{0}$