$p = 3$ 3^2 $a_0 = 0, 1, 2$

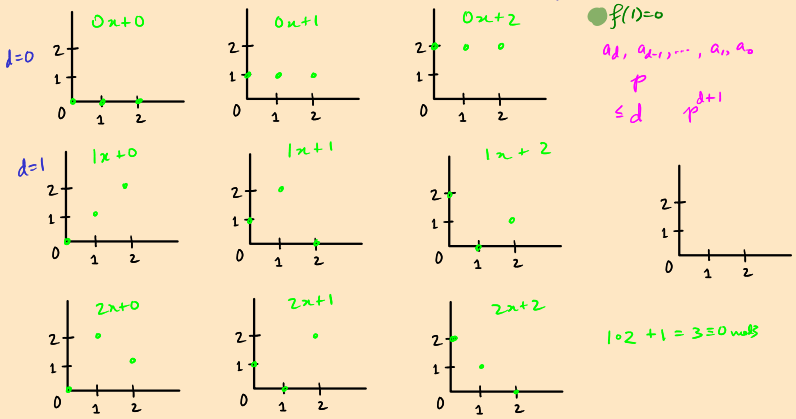
$d \le 1$ 3 choices for a_1, 3 choices for a_0

$d = 1$ $d+1$

$0 \neq a_1 x + a_0$ (2 choices, 3 choices)

$f(1) = 0$

$a_d, a_{d-1}, \dots, a_1, a_0$ p $\le d$ p^{d+1}



$1 \cdot 2 + 1 = 3 \equiv 0 \pmod 3$

2 pts

Given $d+1$ pts, can find a deg $\le d$ poly uniquely.

Because Lagrange Interp.

$p-1$ choices

$d+1-k$

Given k pt

Choose $d+k+1$ more pts.

Do Lagrange Interp.

$p \times p \times \cdots \times p = p^{d+k+1}$ (d times)

$d-k+1$

$\gcd(e, (p-1)(q-1)) = 1$

$d \equiv e^{-1} \pmod{(p-1)(q-1)}$

$de \equiv 1 \pmod{(p-1)(q-1)}$

$de = k(p-1)(q-1) + 1$

e coprime w/ $(p-1)$

$d \equiv e^{-1} \pmod{(p-1)}$

$p = 8$

$e = 3$

$d \equiv 3^{-1} \pmod 7$

$\equiv 5 \pmod 7$

$x = 4$

$(4^3)^5 \equiv (64)^5 \equiv 0^5 \equiv 0 \pmod 8$

$x^{ed} \equiv x \pmod{pq}$

$x^{k(p-1)(q-1)+1} \pmod{pq}$

$x^p \equiv x \pmod p$ (prime)

$x^{p-1} \equiv 1 \pmod p$

$x \not\equiv 0 \pmod p$

CRT

$x^{k(p-1)(q-1)+1} - x \equiv 0 \pmod p$

$x^{k(p-1)(q-1)+1} - x \equiv 0 \pmod q$

$x^{k(p-1)(q-1)+1} - x \equiv 0 \pmod{pq}$

$x^{k(p-1)(q-1)+1} \equiv x \pmod{pq}$

$x \cdot (x^{(p-1)})^{k(q-1)} \pmod p$

$\equiv x \cdot 1^{k(q-1)} \equiv x \pmod p$

$x \cdot 1^{k(p-1)} \equiv x \pmod q$