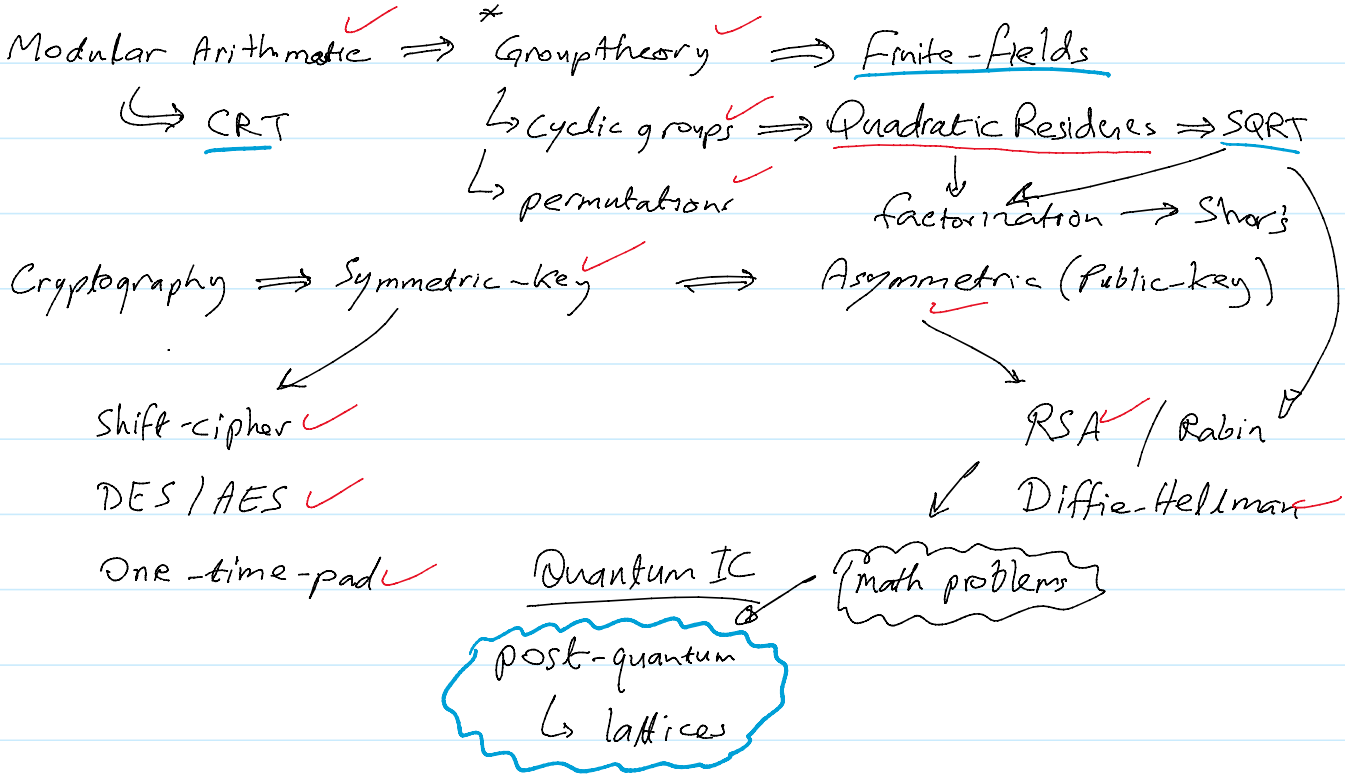
Quadratic Residues

Wednesday, March 24, 2021 8:33 AM

Recall: RSA

Map:



1) Def^n. Let $a \in \mathbb{Z}_n^*$, & q – Forouzan

If $\exists x \in \mathbb{Z}_n^*$, s.t. $x^2 \equiv a \pmod p$

then a is quadratic residue (QR)

else a is quadratic nonresidue (QNR)

e.g.

in $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

4 is QR for $x = 2$, $x^2 \equiv 4 \pmod 7$

for $x = -2 \equiv 5$, $5^2 \equiv 4 \pmod 7$

3 is QNR

2 is QR for $x = 3$, $3^2 \equiv 2 \pmod 7$

for $x \equiv -3 \equiv 4$, $4^2 \equiv 2 \pmod 7$

2] Exer: $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

1 is QR for $x = 1$, $x^2 \equiv 1 \pmod{15}$

also for $x = 14, 4, 11 \Rightarrow x^2 \equiv 1 \pmod{15}$

4 is QR for $x = 2$, $2^2 = 4 \pmod{15}$

also for $x = 8, 13, 7 \Rightarrow x^2 \equiv 4 \pmod{15}$

3] Notation:

$Q_n = \{a \mid a \text{ is QR in } (\bmod n)\}$

$\overline{Q_n} = \{a \mid a \text{ is QNR in } (\bmod n)\}$

4] e.g. $1 \in Q_n \quad \forall n$

$4 \in Q_n \quad \forall n \geq 5$

$3 \in \overline{Q_5}$

$3 \in Q_{11}$ for $x \equiv 5 \Rightarrow x^2 \equiv 3 \pmod{11}$

5] Note: $0 \notin \mathbb{Z}_n^* \Rightarrow 0 \notin Q_n$ and $0 \notin \overline{Q_n}$

6] Thm: if p is an odd prime and $\langle \alpha \rangle = \mathbb{Z}_p^*$, then $\forall a \in \mathbb{Z}_p^*$, $a \in Q_p$ iff $a = \alpha^i$ for even i.

Proof:

for $x = \alpha^{i/2}$ is the root of a, $(\alpha^{i/2})^2 = a$

7] Thm: for odd prime p, $|\mathbb{Z}_p^*| = (p-1)$

$|Q_p| = \frac{p-1}{2}$ and $|\overline{Q_p}| = \frac{p-1}{2}$

$$|Q_p| = \frac{p-1}{2} \quad \text{and} \quad |\bar{Q}_p| = \frac{p-1}{2}$$

8] Thm: if $n = p \cdot q$ where p, q are odd primes, $p \neq q$, then

$a \in Q_n$ iff $a \in Q_p \cap Q_q$

e.g.

$n = 3 \cdot 7 = 21$

① is $a = 13 \in Q_{21}$?

$a = 13$ mod 3 $\Rightarrow a = 1 \in Q_3$

$a = 13$ mod 7 $\Rightarrow a = 6 \in \bar{Q}_7$

$\Rightarrow 13 \in \overline{Q_{21}}$

② is $a = 16 \in Q_{21}$?

$a = 16$ mod 3 $\Rightarrow a = 1 \in Q_3$

$a = 16$ mod 7 $\Rightarrow a = 2 \in Q_7$

$\Rightarrow 16 \in Q_{21}$

9] Thm: Let $n = p \cdot q$, for odd primes p, q

$$|Q_n| = |Q_p| \cdot |Q_q| = \frac{p-1}{2} \cdot \frac{q-1}{2} = \frac{(p-1)(q-1)}{4} = \frac{|\mathbb{Z}_n^*|}{4}$$

e.g. in $\mathbb{Z}_{15}^*$, $|\mathbb{Z}_{15}^*| = \Phi(15) = 8$

$\Rightarrow |Q_{15}| = \frac{8}{2} = 2$ (see Exer [2])

10] Note: by Thm [9], each $a \in Q_n$ has 4 roots

e.g. $16 \in Q_{21} \Rightarrow \sqrt{16} = 4, 17, 10, 11$

e.g. $16 \in Q_{21} \Rightarrow \sqrt{16} = \underbrace{4, 17}_{\pm 4}, \underbrace{10, 11}_{\pm 10}$

Exer: find $\sqrt{1} \pmod{21}$ (HW)

Linear
$x \equiv 1 \pmod{n}$

11] Def^n. The square-root problem (sqrt)
Given $\mathbb{Z}_n^*$, and $a \in \mathbb{Z}_n^*$
find $x = \sqrt{a} \pmod{n}$
i.e. $x^2 \equiv a \pmod{n}$

12] Fact: the sqrt problem is infeasible for composite, without knowing the factors of n.