Crypto Exam Formula Card: Fermat + Miller–Rabin + CRT (with GAP)

1. Setup (always first)

Let:

$$n = pq \quad (p, q \text{ primes})$$

Split everything:

$$x \bmod n \leftrightarrow (x \bmod p,\ x \bmod q)$$

Final count always:

$$\boxed{N = N_p \cdot N_q}$$

GAP check

```
p := 433;; q := 1153;;
n := p*q;;
IsPrime(p); IsPrime(q);
```

—

2. Fermat pseudoprimes

Condition:

$$a^{n-1} \equiv 1 \pmod{n}$$

Count:

$$\boxed{N_p = \gcd(n-1, p-1), \quad N_q = \gcd(n-1, q-1)}$$

$$\boxed{N = \gcd(n-1, p-1) \cdot \gcd(n-1, q-1)}$$

GAP check

```
Gcd(n-1, p-1);
Gcd(n-1, q-1);
```

—

3. Miller–Rabin (only rule you need)

Write:

$$n - 1 = 2^s d \quad (d \text{ odd})$$

Compute:

$$a^d,\ a^{2d},\ a^{4d}, \ldots, a^{2^s d}$$

PASS iff:

$$\boxed{a^d \equiv 1 \ \text{ OR } \ \exists i : \ a^{2^i d} \equiv -1}$$

Otherwise: witness.

GAP check

```
n := 499249;;
Factors(n-1);
```

—

4. Pattern shortcut (MR counting)

If sequence pattern is:

$$*,\ *,\ -1,\ 1$$

Then:

$$a^{4d} \equiv -1, \quad a^{8d} \equiv 1$$

Count in cyclic group of size m:

$$\boxed{\#(x^k = 1) = \gcd(k, m)}$$

So:

$$\boxed{N_p = \gcd(8d, p-1) - \gcd(4d, p-1)}$$

$$\boxed{N_q = \gcd(8d, q-1) - \gcd(4d, q-1)}$$

Final:

$$\boxed{N = N_p N_q}$$

GAP check

```
Gcd(8*d, p-1) - Gcd(4*d, p-1);
Gcd(8*d, q-1) - Gcd(4*d, q-1);
```

—

5. Miller–Rabin Construction $(*, *, -1, 1)$

Goal:

$$*,\ *,\ -1,\ 1 \iff a^{4d} \equiv -1,\ a^{8d} \equiv 1$$

Split:

$$n = pq, \quad \text{solve mod } p \text{ and } q$$

Final:

$$a \equiv a_p \pmod{p}, \quad a \equiv a_q \pmod{q}$$

GAP check

```
ChineseRem([a_p, a_q], [p, q]);
```

—

Step 1: Generator form

Let g generate $(\mathbb{Z}/p\mathbb{Z})^*$:

$$a_p = g^k$$

GAP check

```
g := PrimitiveRootMod(p);
```

—

Step 2: Fix target value

$$g^\ell \equiv -1 \pmod p \quad \Rightarrow \quad \ell = \frac{p-1}{2}$$

GAP check

```
PowerMod(g, (p-1)/2, p);   # should give -1 mod p
```

—

Step 3: Exponent equation

$$4d \cdot k \equiv \ell \pmod{p-1}$$

Solve:

$$k \equiv (4d)^{-1}\ell \pmod{p-1}$$

Then:

$$a_p = g^k$$

Repeat for q.

GAP check

```
k := (4*d)^-1 * ((p-1)/2) mod (p-1);
PowerMod(g, k, p);
```

—

Step 4: Combine

$$a \equiv a_p \pmod p, \quad a \equiv a_q \pmod q$$

—

Step 5: Second solution

If a works, then:

$$n - a$$

also works.

GAP check

```
PowerMod(n-a, 4*d, n);
```

—

Workflow summary

- write $a = g^k$
- replace -1 by $(p-1)/2$
- solve $4dk \equiv (p-1)/2$
- build a_p, a_q
- CRT