Recall: the discrete log problem: given prime p, $b \in \{1, 2, \dots, p-1\}$ and $a \equiv b^x \pmod{p}$, find x.

For the problem to be difficult we need:

- $\operatorname{ord}_p(b)$ to be large (prefferably, b should be a primitive root).
- p should be large.

There is an algorithm (Pohling-Hellman) which can quickly find x if all prime divisors of $\operatorname{ord}_p(b)$ are small. (go through it later).

- $\operatorname{ord}_p(b)$ should have a large prime divisor $\Rightarrow$ the same should happen for $p-1$.

Note: $p-1$ is even (for $p \geq 3$) $\Rightarrow$ $p-1 = 2q$. Ideally, we want to find p such that q is prime.

Definition: A prime p is called safe if $p = 2q+1$ and q is prime (Sophie-German prime).

§16 Safe primes.

Table of the first safe primes:

q	2	3	5	11	23	29	41	53	...
$p=2q+1$	5	7	11	23	47	59	83	107	

Conjecture: there are infinitely many safe primes.

Note: ~~For~~ Every prime $p \neq 2$ is either $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$.
$\Rightarrow$ Every safe prime $p \neq 5$ is $\equiv 3 \pmod 4$.

Proposition: There are infinitely many primes $p \equiv 3 \pmod 4$.

Proof: Suppose there are finitely many of them: $p_1, p_2, \dots, p_k$.

Consider $R = 4 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k - 1$

R is not divisible by any p_i.

$R \equiv 3 \pmod 4$

All prime factors of R are $\equiv 1 \pmod 4$ or 2.

Their product $(=R)$ is $\equiv 1, 2, 0 \pmod 4$

Contradiction $\boxtimes$

Proposition: There are infinitely many primes $\equiv 1 \pmod 4$.

Proof. Suppose there are finitely many of them: $p_1, p_2, \dots, p_k$.

Consider $S = (4 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k)^2 + 1$

S is not divisible by $2, p_1, p_2, \dots, p_k$.

Take any prime $q \mid S$. Then $q \equiv 3 \pmod 4$

Then $x = 4 \cdot p_1 \cdot \dots \cdot p_k$ is a solution of

$$x^2 + 1 \equiv 0 \pmod q \iff x^2 \equiv -1 \pmod q.$$

However from the result from lectures we know that $x^2 \equiv -1 \pmod q$ does not have solutions if $q \equiv 3 \pmod 4$. Contradiction. $\boxtimes$

Q: How many safe primes with k bits do we have?

Heuristic: Prime Number Theorem:

$$\#\{\text{primes} \leq N\} \sim \frac{N}{\ln N}$$

ratio $\to 1$ as $N \to \infty$.

$$\Rightarrow \#\{\text{primes with } k \text{ bits}\} \sim \frac{2^k}{k \ln 2} - \frac{2^{k-1}}{(k-1)\ln 2}$$

$$= \frac{(k-2) \cdot 2^{k-1}}{k(k-1)\ln 2} \sim \frac{2^{k-1}}{k \ln 2}.$$

$\Rightarrow$ Probability that k-bit number is prime is $\sim \frac{1}{k \ln 2}$.

Probability that k-bits odd number is prime is $\sim \frac{2}{k \ln 2}$.

Incorrect assumption: $\{p$ is prime$\}$ and $\{\frac{p-1}{2}$ is prime$\}$ are independent.

Note: if p has k bits then $\frac{p-1}{2}$ has $k-1$ bits.

Then the probability that odd p and $\frac{p-1}{2}$ are both primes is

$$\sim \frac{2}{k \ln 2} \cdot \frac{1}{(k-1) \ln 2} \sim \frac{2}{k^2 (\ln 2)^2}.$$

By using more advanced techniques we get the probability

$$\sim C \cdot \frac{2}{k^2 (\ln 2)^2} \quad \text{with } C = \prod_{p \text{ prime} \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.6606\ldots$$

Conclusion: If we want to find a safe 600-digit prime, we will have to do up to 10^5-10^6 checks.

If p is a safe prime, what can we say about $ord_p(b)$ for various b?

$p-1=2q \Rightarrow ord_p(b) \in \{1, 2, q, 2q\}$.

$ord_p(b) = 1 \Rightarrow b \equiv 1 \pmod p$

$ord_p(b) = 2 \Rightarrow b^2 \equiv 1 \pmod p \Rightarrow b \equiv \pm 1 \pmod p$.

Other values of b give $ord_p(b) \in \{q, 2q\}$.

They can be used in cryptography.