Definition 1 (Euler φ function) For every $n \in \mathbb{N}$, $\varphi(n) = |\{a \in \mathbb{N} : a \leq n \text{ and } (a, n) = 1\}|$.

Theorem 1 (Fermat's Little Theorem)

$$p \text{ prime and } (a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}.$$

Proof Use Lagrange's theorem on finite group $\mathbb{F}_p^*$.

Definition 2 (Witness) An integer a such that $a^p \not\equiv a \pmod{p}$

Definition 3 (Carmichael Number) An integer N such that $a^N \equiv a \pmod{N}$ and N is composite.

Example $561 = 3 \cdot 11 \cdot 17$.

Miller-Rabin: Work in $\mathbb{F}_p^*$ (cyclic order $p-1$). Write $p - 1 = 2^k m$. Then for every $a \in \mathbb{F}_p^*$ either $a^m = 1$ or $\exists j : a^{2^j m} = -1$. This follows from Fermat's little theorem, as each number for different j is square of the precedent and the last is congruent to 1 (write list). Miller-Rabin witness. Then the Miller-Rabin test select random a and test N. If N is composite, then there is at least $3(N-1)/4$ witnesses (theorem by Shoup) $\approx 75\%$. If select $\log(N)$ possible bases a, then complexity[1] $\mathcal{O}(\log(N)^4)$ or $\mathcal{O}(\log(N)^2 M(\log(N)))$ for multiplication cost M.

Definition 4 (B-smoothness) An integer $N = \prod p_i^{e_i}$ is B-smooth if $\forall i \ p_i \leq B$. It is B-powersmooth if $\forall i \ p_i^{e_i} \leq B$.

Pollard $p-1$ (1974): Suppose $N = pq$. If $p-1$ is B-powersmooth and $q-1$ is not (for some B) then there is a good chance that $p-1$ divides $B!$ and $q-1$ doesn't. This means that, for random a, p divides $a^{B!} - 1$ (or equivalently $a^{B!} \equiv 1 \pmod{p}$) [2] and so can retrieve factor p by $(a^{B!} - 1, N)$. Lesson learned: careful when choosing p and q. Complexity $\mathcal{O}(B \log(B) M(\log(N)))$ thus exponential in B. So useful only for small B.

Definition 5 (Sophie-Germain Primes) A prime number p such that $p' = 2p+1$ is also prime.

Also known as Safe Primes, Conjectured infinitely many. Example 11.

Remark 1 Most efficient method of this type uses Elliptic Curves (maybe see after). All of these methods hardest for p, q same size as smallest factor $\approx \sqrt{N}$.

Definition 6 (Factor Base) The set $\mathcal{B} = \{p_1, \ldots, p_s\}$ of all the prime numbers less than B.

[1] All complexities are in bit operations.

[2] check exercise using Fermat's little Theorem

Random Squares (Dixon): Suppose $N = a^2 - b^2$. Then trivial to factor N. So look for b such that $N + b^2 = a^2$. Better to look for $kN + b^2 = a^2$, or, equivalently, $a^2 \equiv b^2 \pmod{N}$ and then compute $(a + b, N)$ and $(a - b, N)$. Choose a factor base $\mathcal{B} = \{p_1, \ldots, p_s\}$ and random $x < N$, then compute $y = x^2 \pmod{N}$. If y is B-smooth then it factors over $\mathcal{B}$. Save the exponent vector $\eta = (e_1, \ldots, e_s)$. Repeat for other values of x until you have a good number t of relations. Then can use a linear combination λ of the x to obtain exponent vectors that are $(0, \ldots, 0) \pmod{2}$. Set $\sum_{j=1}^{t} \lambda_j \eta_j = (2f_1, \ldots, 2f_s)$ and construct $a = \prod_{j=1}^{t} x_j{}^{\lambda_j} \pmod{N}$ and $b = \prod_{i=1}^{s} p_i{}^{f_i} \pmod{N}$. It is clear that $a^2 \equiv b^2 \pmod{N}$.

Definition 7 (Subexponential Function) Let $0 \leq \alpha \leq 1$ and $\beta \in \mathbb{R}^+$. The function

$$L_N(\alpha, \beta) = e^{\beta \log(N)^{\alpha} \log(\log(N)^{1-\alpha})}.$$

Observe $\alpha = 0 \Rightarrow \log(N)^{\beta}$ *(polynomial) and* $\alpha = 1 \Rightarrow N^{\beta}$ *(exponential).*

Claim 1 *The complexity of random squares method is* $L_N(1/2, 2 + o(1))$.

Hence independent of size of factors.

Quadratic Sieve (Pomerance): Start from Eratosthenes (III sec.) and adapt by dividing. We use a factor base $\mathcal{B} = \{p_1, \ldots, p_s\}$. Let $m = \lfloor \sqrt{N} \rfloor + 1$ and consider the polynomial $f(x) = x^2 - N$. Calculate $y_i = f(m + i)$ for $i = 0, 1, 2, \ldots$ and check if is B-smooth: this is done by sieving as mentioned before (use example) by checking $(m + i)^2 \equiv N \pmod{p_i}$. Either two solutions a_{p_i}, b_{p_i} or none. If solutions, sieve every p_i-th entry in the list starting from $f(a_{p_i})$ and $f(b_{p_i})$. For each of these y_i we can then store the exponent vector and proceed as above.

We construct the factor base accordingly, using also prime powers.

Claim 2 *The (heuristic) complexity of the quadratic sieve is* $L_N(1/2, 1 + o(1))$.