Another principle to factor

Example. Factor 8051

$$8051 = 8100 - 49 = 90^2 - 7^2$$
$$= (90+7)(90-7) = 97 \cdot 83. \quad \lrcorner$$

Prop. 6.8. $x \not\equiv \pm y \pmod n$, $x^2 \equiv y^2 \pmod n$
$\Rightarrow \gcd(x-y, n)$ is a nontrivial divisor of n. $\lrcorner$

Proof. $x^2 \equiv y^2 \pmod n$, i.e., $n \mid x^2 - y^2$.
Hence $n \mid (x+y)(x-y)$. By assumption $n \nmid (x-y)$ and $n \nmid (x+y)$, which shows the assumption. ∎

- Prop. 6.8. forms the basis of "quadratic sieve factoring". Problem: determine x, y satisfying the assumptions of §6.8.
  [see Stinson (2002), p. 182-194]
- $\gcd(a,b)$ can be eff. computed. → later sect 6.3.

Factoring in practice

The most successful methods for factoring

- quadratic sieve
- elliptic curve factorization
- number field sieve (most powerful)

All are "subexponential", however, non polynomial.

History

1994:	RSA-129	Atkins et. al. quadr. sieve, 600 workstations
1996:	RSA-130	
1999:	RSA-155	8400 MIPS, 300 PCs
2003:	RSA-174	
2005:	RSA-193	5 months, 80 2.2 GHz Opteron CPU (BSI)
2010:	RSA-232	"many" hundreds of 2.2 GHz CPU almost 2 years.

Factoring is considered a one-way function.

6.3. The Extended Euclidean Algorithm

Known: $\gcd(a,n) = 1 \Rightarrow \exists$ inverse s with $a \cdot s \equiv 1 \pmod{n}$

Aim: efficient algorithm to compute $s = a^{-1} \pmod{n}$.

Euclidean Alg. Let $r_0 > r_1 \in \mathbb{N}$

$r_0 = q_1 r_1 + r_2$, $0 < r_2 < r_1$	$r_2 = r_0 - q_1 r_1 = s_2 r_0 + t_2 r_1$
$r_1 = q_2 r_2 + r_3$, $0 < r_3 < r_2$	$r_3 = r_1 - q_2 r_2 = s_3 r_0 + t_3 r_1$
$\vdots$	$\vdots$
$r_{k-2} = q_{k-1} r_{k-1} + r_k$, $0 < r_k < r_{k-1}$	$r_k = s_k r_0 + t_k r_1$
$r_{k-1} = q_k r_k$	

It holds that $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{k-1}, r_k) = r_k$

[Since $\gcd(a,b) = \gcd(b, a - qb)$]

If $\gcd(r_0, r_1) = 1$, then $s_k r_0 + t_k r_1 = 1$

$\Rightarrow t_k r_1 \equiv 1 - s_k r_0 \equiv 1 \pmod{r_0}$, i.e.

$t_k \equiv r_1^{-1} \pmod{r_0}$

Define recursively

$t_0 = 0,\ t_1 = 1,\ t_j = (t_{j-2} - q_{j-1} t_{j-1}) \bmod r_0,\ j \geq 2$

Theorem 6.8. $r_j \equiv t_j \cdot r_1 \pmod{r_0}$ $\quad j = 0, \dots, k$

Proof. (by induction on j)

$j=0$: $r_0 \equiv t_0 r_1 \pmod{r_0}$ ✓

$j=1$: $r_1 \equiv t_1 r_1 \pmod{r_0}$ ✓

$(j-2, j-1) \mapsto j$:

$$r_j \overset{\text{Eucl. alg.}}{=} r_{j-2} - q_{j-1} r_{j-1}$$

$$\overset{\text{I.V.}}{\equiv} t_{j-2} r_1 + q_{j-1} t_{j-1} r_1$$

$$\equiv (t_{j-2} - q_{j-1} t_{j-1}) r_1 \equiv t_j r_1 \pmod{r_0}$$ ∎

Corollary 6.9. $\gcd(r_0, r_1) = 1 \Rightarrow t_k \equiv r_1^{-1} \pmod{r_0}$ ⌟

Number of divisions in the Eucl. alg.

$$\leq \log_\phi(\sqrt{5}\, r_0) - 2, \quad \underbrace{\phi = \tfrac{1}{2}(1+\sqrt{5})}_{\text{golden ratio}}$$

Least favorable case if r_0, r_1 are successive Fibonacci numbers:

1 1 2 3 5 8 13 21 ...

(cf. Knuth II, Chap. 4.5.3, p. 320)

Implementation: Stinson (2002) p. 161

6.4. The Chinese Remainder Theorem (CRT)

Method for solving systems of congruences.

Theorem 6.10. (CRT)

Suppose $m_1, \dots, m_r$ are pairwise relatively prime, $a_1, \dots, a_r \in \mathbb{N}$. The system of r congruences

$$x \equiv a_i \pmod{m_i}, \quad i = 1, \dots, r.$$

has a unique solution modulo $M = m_1 \cdots m_r$, given by

$$x = \sum_{i=1}^{r} a_i M_i y_i \mod M,$$

where $M_i = M/m_i$, $y_i = M_i^{-1} \bmod m_i$, $i = 1, \dots, r$.

Proof. Stinson (02), p. 162, 163. ∎

Example: $r = 3$, $m_1 = 7$, $m_2 = 11$, $m_3 = 13$

$\Rightarrow M = 1001$, $M_1 = 143$, $M_2 = 91$, $M_3 = 77$

$y_1 = 143^{-1} \bmod 7 = 3^{-1} \bmod 7 = 5$

$y_2 = 4$, $y_3 = 12$

Solution of $x \equiv 5 \pmod 7$ $(a_1 = 5)$

$x \equiv 3 \pmod{11}$ $(a_2 = 3)$

$x \equiv 10 \pmod{13}$ $(a_3 = 10)$

is $x = 5 \cdot 143 \cdot 5 + 3 \cdot 91 \cdot 4 + 10 \cdot 77 \cdot 12 \bmod 1001$

$= 894$.

7. The Discrete Logarithm & Related Cryptosystems

Def. 7.1. Let $a \in \mathbb{Z}_n^*$ $(a \neq 0, \gcd(a,n)=1)$

$$\mathrm{ord}_n(a) = \min\{k \in \{1,\dots,\varphi(n)\} \mid a^k \equiv 1 \pmod n\}$$

is called the order of a modulo n.

a is called a primitive element modulo n (PE) if $\mathrm{ord}_n(a) = \varphi(n)$. ⊿

Idea behind this definition.

$|\mathbb{Z}_n^*| = \varphi(n)$. If $a \in \mathbb{Z}_n^*$ is PE mod n then

$a^1 \bmod n$, $a^2 \bmod n$, ..., $a^{\varphi(n)} \bmod n \in \mathbb{Z}_n^*$

$\not\equiv 1$ $\not\equiv 1$ $\equiv 1$

Suppose that $\exists\, 1 \le i < j \le \varphi(n) : a^i \equiv a^j \pmod n$

Then $a^{j-i} \equiv 1 \pmod n$, a contradiction.

Hence $\{a^1 \bmod n, a^2 \bmod n, \dots, a^{\varphi(n)} \bmod n\} = \mathbb{Z}_n^*$

$\mathbb{Z}_n^*$ is generated by powers of a.

Such groups are called cyclic. a is called generator.

Problem: Is there always a PE mod n?

Theorem 7.2 a) There exists a PE mod n iff

$$n \in \{2, 4, p^k, 2p^k \mid p \geq 3 \text{ prime}, k \in \mathbb{N}\}$$

b) If PE mod n exists, then there are $\varphi(\varphi(n))$ many. ⊥

Particularly, if $n = p$ prime

$$\exists\, a \in \mathbb{Z}_p^* : \mathbb{Z}_p^* = \{a^k \mid k = 1, \dots, p-1\}$$

Example. $n = 7$, $\varphi(n) = 6$. Determine all PE mod 7

	powers mod 7
$a=2$	$2, 4, 8 \equiv 1 \pmod 7$ → no PE
$a=3$	$3, 9 \equiv 2, 27 \equiv 6, 81 \equiv 4, 243 \equiv 5, 729 \equiv 1 \pmod 7$ → PE
$a=5$	$5, 25 \equiv 4, 125 \equiv 6, 625 \equiv 2, 3125 \equiv 3, 15625 \equiv 1 \pmod 7$ → PE

It holds that $\varphi(\varphi(7)) = \varphi(6) = |\{1, 5\}| = 2$

Hence, 3, 5 are the only PE mod 7. ⊥