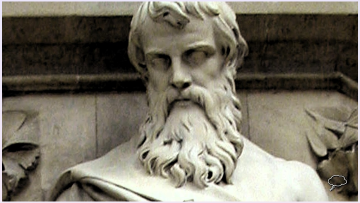
Foundations of public key cryptography

Dr. Dmitry Gokhman

Department of Mathematics

2019 April 12

gokhman@math.utsa.edu
http://zeta.math.utsa.edu/∼gokhman



Euclid ($\varepsilon\upsilon\kappa\lambda\varepsilon\iota\delta\eta\varsigma$), Alexandria, Egypt ($\approx$ 300 BC)

Division algorithm:

$$\forall a, b \in \mathbf{Z}, b > 0 \quad \exists! q, r \in \mathbf{Z} \quad a = qb + r, \quad 0 \leq r < b.$$

Let $r = \min\{a - kb \geq 0 \colon k \in \mathbf{Z}\} = a - qb.$

$$a - (q+1)b = a - qb - b = r - b \quad \Rightarrow \quad r < b.$$

Claude-Gaspard Bachet de Meźiriac, Savouè (1581–1638)

Étienne Bézout, France (1730–1783)

Bézout's identity

$$\forall a, b \in \mathbf{N} \quad \exists s, t \in \mathbf{Z} \quad \gcd(a, b) = sa + tb.$$

Let $d = \min\{sa + tb > 0 \colon s, t \in \mathbf{Z}\}$.

Any common divisor of a, b divides d.

Division algorithm $\Rightarrow$ d is a common divisor of a, b.

(if $a = qd + r$, $r = a - q(sa + tb) = (1 - qs)a - qtb$. and since $r < d$, $r = 0$)

Euclid's algorithm

$\gcd(35, 74) = 1$

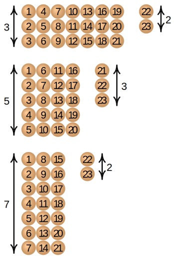
long-divide, replace with remainder and divide the other way until you get clean division

$$74 = 2 \cdot 35 + 4$$
$$35 = 8 \cdot 4 + 3$$
$$4 = 3 + 1$$

... extended

solve for remainders, substitute and collect terms

$$4 = 74 - 2 \cdot 35$$
$$3 = 35 - 8 \cdot 4$$
$$1 = 4 - 3 = 4 - (35 - 8 \cdot 4) = 9 \cdot 4 - 35 = 9(74 - 2 \cdot 35) - 35 = 9 \cdot 74 - 19 \cdot 35$$



Carl Friedrich Gauss (Princeps Mathematicorum), Braunschweig (1777-1855)

Modular arithmetic

Pick $m \in \mathbf{Z}$, $m > 1$ (modulus).

For $i, j \in \mathbf{Z}$ define congruence $i \equiv j \bmod m \;\Leftrightarrow\; i - j \in m\mathbf{Z}$.

Congruence is an equivalence relation. Congruence classes (cosets of $m\mathbf{Z}$) partition $\mathbf{Z}$ and form the factor ring $\mathbf{Z}_m = \mathbf{Z}/m\mathbf{Z}$.

Example

$\mathbf{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

$[0]_3 = 3\mathbf{Z} = \{\ldots -3, 0, 3, 6, 9\ldots\}$
$[1]_3 = 1 + 3\mathbf{Z} = \{\ldots -2, 1, 4, 7, 10\ldots\}$
$[2]_3 = 2 + 3\mathbf{Z} = \{\ldots -1, 2, 5, 8, 11\ldots\}$

Units

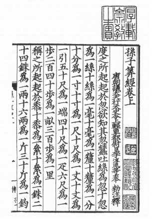
By Bézout's identity $[k]_m \in \mathbf{Z}_m$ is a unit (has a multiplicative inverse) $\Leftrightarrow \gcd(k, m) = 1 \Leftrightarrow \mathbf{Z}_m = \langle k \rangle$.

The multiplicative group of all units in $\mathbf{Z}_m$ is denoted $U(m)$.

Modular power algorithm

expand the exponent in binary, split up the task, reduce mod m at each step

$25^{11} = 25^{1+2+8} = 25 \cdot 25^2 \cdot 25^3$



孫子筭經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勅注釋

度之所起起於忽欲知其忽蠶吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一絫十絫爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

Sun Tzu (孫武), Zhou (544 BC – 496 BC)

If $\gcd(m,n) = 1, \quad \mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$.

(generalizes to finite products of ring with pairwise co-prime moduli)

Define additive homomorphism $\psi\colon \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\psi([k]_{m,n}) = ([k]_m, [k]_n)$.

If $\psi([k]_{mn}) = 0$, k is a common multiple of m and n, so $\mathrm{lcm}(m,n)$ divides k.

Recall $\gcd(m,n) \cdot \mathrm{lcm}(m,n) = mn$. If $\gcd(m,n) = 1, \mathrm{lcm}(m,n) = mn$.

Thus $k = [0]_{mn}$, so $\ker\psi$ is trivial, so ψ is one-to-one.

Since the sizes of domain and target are both mn, ψ is also onto.

Explicit formula (compositional inverse of ψ)

Suppose $x \equiv b_i \bmod m_i$, where $m_i (1 \le i \le n)$ are pairwise co-prime moduli.

$$x = \sum_{i=1}^{n} M_i \, (M_i^{-1} \bmod m_i) \, b_i \quad \bmod m$$

where $m = \prod_{i=1}^{n} m_i$ and $M_i = \frac{m}{m_i} = \prod_{j \neq i} m_j$ $\qquad (\psi(x) = [b_1, \ldots b_n])$

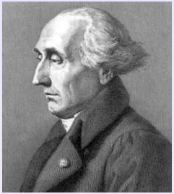
$x \equiv 3 \bmod 5$
$x \equiv 4 \bmod 7$
$x \equiv 5 \bmod 11$

$m = 5 \cdot 7 \cdot 11 = 385$

i	m_i	$M_i = \frac{m}{m_i}$	$y_i = M_i^{-1} \equiv \bmod m_i$	a_i	$M_i y_i a_i$
1	5	77 $\equiv 2 \bmod 5$	3 $(3 \cdot 2 = 5 + 1)$	3	693 $\equiv 308 \bmod 385$
2	7	55 $\equiv 6 \bmod 7$	6 $(6 \cdot 6 = 5 \cdot 7 + 1)$	4	1320 $\equiv 165 \bmod 385$
3	11	35 $\equiv 2 \bmod 11$	6 $(6 \cdot 2 = 11 + 1)$	5	1050 $\equiv 280 \bmod 385$

$165 + 280 \equiv 60 \bmod 385$

Sum: $368 \bmod 385$

Pierre de Fermat, Toulouse, France (1607–1665)

Leonhard Euler, Basel (1707–1783)

Joseph-Louis (Giuseppe-Luigi) Lagrange, Piemonte (1736–1813)

Euler's totient $\varphi(m) = |U(m)| = |\{0 < k < m \colon \gcd(k, m) = 1\}|$

If p is prime, $\varphi(p^k) = p^k - p^{k-1}$. (Eliminate powers of p^j for $j < k$)

If $\gcd(m, n) = 1$, $U(mn) = U(m) \times U(n)$, so $\varphi(mn) = \varphi(m)\varphi(n)$.

$([k]_m, [k]_n) \in \mathbf{Z}_m \times \mathbf{Z}_n$ is a unit $\Leftrightarrow$ both $[k]_m$ and $[k]_n$ are units.

If $\gcd(m, n) = 1$, ψ is an isomorphism, so preserves units.

E.g. $\varphi(12) = \varphi(4 \cdot 3) = \varphi(4)\varphi(3) = (4-2)(3-1) = 4$, $U(12) = \{1, 5, 7, 11\}$

Lagrange's theorem

Given a finite group G and $H < G$, define an equivalence $x \sim y \Leftrightarrow xy^{-1} \in H$. Equivalence classes (cosets xH of H) partition G.

Since $|xH| = |H|$, $|G| = |H| \cdot [G : H]$, where $[G : H] = \#(\text{cosets})$.

In particular, if $x \in G$, $|x| = |\langle x \rangle|$ divides $|G|$, so $x^{|G|} = e_G$.

Euler's theorem: if $k \in U(m)$, $k^{\varphi(m)} \equiv 1 \bmod m$.

Fermat's little theorem: if $k \in \mathbf{Z}_p$, $k \neq 0$, $k^{p-1} \equiv 1 \bmod m$.

(so if $k \in \mathbf{Z}_p$, $k^p \equiv k \bmod m$)

1973 Clifford Cocks

1977 RSA: Ronald Rivest, Adi Shamir, Leonard Adleman

Key pair generation

Pick two large primes $p \neq q$ and let $n = pq$. Then $\varphi(n) = (p-1)(q-1)$.
Pick e co-prime to $\varphi(n)$ (so e is a unit).
Use extended Euclid's algorithm to find its inverse $d \in U(n)$.

Public key: $[n, e]$ Secret Key: d

Encoding of message m: $c \equiv m^e \bmod n$

Decoding: $m \equiv c^d \bmod n$

Euler's theorem $\Rightarrow (m^e)^d = m^{ed} = m^{1+k\varphi(n)} = m \cdot (m^{\varphi})^k = m \pmod{n}$

Key pair generation

```
(%i6)   /* pick 2 distinct primes */
        p:2^1279-1;
        q:2^2203-1;
        n:p*q;

        /* pick encoding key to publish along with n */
        e:1234786123;
        /* check that e is a unit */
        gcd(e,(p-1)*(q-1));

        /* secret decoding key */
        d:inv_mod(e,(p-1)*(q-1));
(p)     104079321946643990819252403273[326 digits]186900714720710555703168729087
(q)     147597991521418023508489862273[604 digits]809865681250419497686697771007
(n)     153618988782356965746670001051[989 digits]052888831678087029867946180609
(e)     1234786123
(%o5)   1
(d)     280178879675717298364586053315[988 digits]649032687971255315973416277747
```

Encoding

```
(%i8)   /* message */
        m:404;

        /* coded c=m^e mod n */
        c:power_mod(m,e,n);
(m)     404
(c)     501713064691106274378556837138[988 digits]865760982252638435485589364626
```

Decoding

```
(%i9)   power_mod(c,d,n);
(%o9)   404
```