MPRI – Cours 2-12-2

F. Morain

Lecture I: Groups for cryptology (part I)

2013/09/23–30

Before I forget...

- Algorithmic number theory is about algorithms of number theory and they need to be practiced (Maple, Magma, SAGE, pari-gp, etc.).
- A large part of my lectures is taken from a nearly finished book with J.-L. Nicolas.

Plan

I. Elementary arithmetic.

II. $\mathbb{Z}/N\mathbb{Z}$, $(\mathbb{Z}/N\mathbb{Z})^*$.

III. Quadratic reciprocity.

IV. Finite fields.

V. Implementation issues.

Good reading

- G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Clarendon Press, 5th edition, 1985.
- D. E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms*. Addison-Wesley, 2nd edition, 1981.
- H. Cohen. *A course in algorithmic algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 4th printing, 2000.
- P. Ribenboim. *The new book of prime number records*. Springer-Verlag, 1996.
- R. Crandall and C. Pomerance. *Primes – A Computational Perspective*. Springer Verlag, 2nd edition, 2005.
- FM. La primalité en temps polynomial [d'après Adleman, Huang; Agrawal, Kayal, Saxena]. Séminaire Bourbaki, Mars 2003.

I. Elementary arithmetic

A) Divisibility

Thm.[Euclidean Division] $\forall\, a, b \neq 0$, $\exists$ a unique pair (q, r) s.t.

$$a = bq + r, \quad 0 \leq r < |b|.$$

Coro. $\mathbb{Z}$ is principal: all proper ideal of $\mathbb{Z}$ are $a\mathbb{Z}$ for $a \in \mathbb{N}^*$.
Def. $b \mid a$ iff $\exists c$, $a = bc$; otherwise $b \nmid a$.
Prop. The following are equivalent

1. $b \mid a$;
2. the remainder of the euclidean division of a by b is 0;
3. $a\mathbb{Z} \subset b\mathbb{Z}$.

Prop.

1. $(d \mid a$ and $d \mid b) \Rightarrow d \mid (\lambda a + \mu b)$;
2. $(d \mid b$ and $b \mid a) \Rightarrow d \mid a$;
3. $a \mid b \Rightarrow |a| \leq |b|$.

Gcd, Lcm

Prop. $a\mathbb{Z} + b\mathbb{Z} = \{au + bv, u \in \mathbb{Z}, v \in \mathbb{Z}\} = d\mathbb{Z}$ with $d > 0$ (greatest common divisor – gcd).
Prop.

$$d = \gcd(a, b) = \max \mathcal{D}(a) \cap \mathcal{D}(b),$$

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d).$$

Prop. $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ with $m > 0$ (least common multiple – lcm).
Prop. $a\mathbb{Z} \cap b\mathbb{Z} =$ set of common multiples of a and b.

$$\begin{array}{ll}
\gcd(a,b) = \gcd(b,a), & \operatorname{lcm}(a,b) = \operatorname{lcm}(b,a) \\
\gcd(a,a) = a, & \operatorname{lcm}(a,a) = a \\
\gcd(a,0) = a, & \operatorname{lcm}(a,0) = 0 \\
\gcd(a,-b) = \gcd(a,|b|), & \operatorname{lcm}(a,-b) = \operatorname{lcm}(a,|b|) \\
\gcd(ca,cb) = c\ \gcd(a,b), & \operatorname{lcm}(ca,cb) = c\ \operatorname{lcm}(a,b).
\end{array}$$

Def. a and b are prime together iff $\gcd(a, b) = 1$.
Rem. if $d = \gcd(a, b)$, then a/d and b/d are prime together.

Euclid's algorithm

Prop. If $a = bq + r$, with $0 \leq r < b$, then $\gcd(a, b) = \gcd(b, r)$.
Proof :

Define (q_i) and (r_i):

$$\begin{array}{ll}
a = bq_1 + r_1, & 0 \leq r_1 < b \\
b = r_1 q_2 + r_2, & 0 \leq r_2 < r_1 \\
\ldots & \\
r_i = r_{i+1} q_{i+2} + r_{i+2}, & 0 \leq r_{i+2} < r_{i+1}
\end{array}$$

(r_i) is strictly decreasing: let k s.t. $r_k = 0$. Then $\gcd(a, b) = r_{k-1}$.

Euclid (cont'd)

Prop. The number of divisions is $\leq 2 \log b / \log 2 + 1$.

Thm. (Knuth) a, b uniformaly in $[1, N]$. Then

1. the number of steps is

$$\left\lceil \frac{\log(\sqrt{5}N)}{\log((1+\sqrt{5})/2)} \right\rceil - 2 \approx \lceil 2.078 \log N + 1.672 \rceil - 2;$$

2. the average number of steps is

$$\frac{12 \log 2}{\pi^2} \log N + 1.47 \approx 0.843 \log N + 1.47.$$

Bézout

There exist u, v s.t.

$$au + bv = \gcd(a, b).$$

Define (u_i), (v_i) s.t. $u_{-1} = 1, v_{-1} = 0, u_0 = 0, v_0 = 1$, and for $-1 \leq i \leq k-2$,

$$\begin{cases} u_{i+2} = u_i - q_{i+2}u_{i+1} \\ v_{i+2} = v_i - q_{i+2}v_{i+1} \end{cases}$$

$$u_1 = 1, v_1 = -q_1, u_2 = -q_2, v_2 = 1 + q_1q_2$$

Lem. For $-1 \leq i \leq k$, $r_i = u_ia + v_ib$.
$\Rightarrow$ take $u = u_{k-1}$ and $v = v_{k-1}$.

Thm. (Bachet-Bézout) $\gcd(a, b) = 1$ iff $\exists$ u, v s.t. $au + bv = 1$.

Gauss lemma

Thm. (Gauss) Let $\gcd(a, b) = 1$, c an integer: $a \mid bc \Rightarrow a \mid c$.
Proof:

Thm. $\gcd(a, b) = 1 \Rightarrow \mathrm{lcm}(a, b) = |ab|$.
Proof:

Coro. $\gcd(a, b)\mathrm{lcm}(a, b) = |ab|$.
Proof:

B) Prime numbers

Def. prime number: p s.t. $\mathrm{Card}\mathcal{D}(p) = 2$; if not prime, then composite.
Smallest primes: $2, 3, 5, 7, 11, 13, \ldots$
Thm. the integer n has at least one prime factor p.
Proof:

Coro. if n is composite, n has at least one prime factor $p \leq \sqrt{n}$.
Proof:

Thm. (Euclide) There exists an infinite number of primes.
Proof:

Thm. (Gauss) If $p \mid a_1a_2 \cdots a_n$, there is some i s.t. $p \mid a_i$.
Proof: (recurrence)

Coro. Let p be prime and $1 \leq k \leq p-1$. Then $p \mid \binom{p}{k}$.
Proof:

Factoring into primes

Thm. For all integer n:

$$n = \varepsilon p_1p_2 \ldots p_k$$

where $\varepsilon = \pm 1$ and $p_1 \leq p_2 \leq \cdots \leq p_k$ are prime numbers.
Proof: (reccurence on n)

Notation. Sometimes

$$n = \varepsilon p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

with $p_1 < p_2 < \cdots < p_k$ and $\alpha_i > 0$.

Valuations

p-adic valuation: For p prime, $\nu_p(n)$ = largest integer s.t. $p^{\nu_p(n)} \mid n$.

$$n = \varepsilon \prod_{p \in \mathbb{P}} p^{\nu_p(n)}.$$

Prop.

1. $\nu_p(ab) = \nu_p(a) + \nu_p(b)$;
2. $a \mid b \Leftrightarrow (\forall p \in \mathbb{P}) \nu_p(a) \leq \nu_p(b)$.

Prop.

$$a = \prod_{p \in \mathbb{P}} p^{\nu_p(a)}, \quad b = \prod_{p \in \mathbb{P}} p^{\nu_p(b)}$$

$\Rightarrow$

$$\gcd(a, b) = \prod_{p \in \mathbb{P}} p^{\min(\nu_p(a), \nu_p(b))},$$

$$\operatorname{lcm}(a, b) = \prod_{p \in \mathbb{P}} p^{\max(\nu_p(a), \nu_p(b))}.$$

Estimates on prime numbers

Thm. (Hadamard, de la Vallée Poussin)
$\pi(x) = \#\{N \leq x, N \text{ is prime}\} \approx x/\log x$.

Thm. (Rosser & Schoenfeld)

$$\frac{x}{\log x}\left(1 + \frac{1}{2\log x}\right) < \pi(x) < \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right)$$

for $x \geq 59$.

Thm. (See Ellison + Mendès France)
$\pi(x; k, \ell) = \#\{N \leq x, N = kn + \ell \text{ is prime}\} \sim \frac{x}{\varphi(k)\log x}$.

Rem. A fast way to compute exact (small) values of $\pi(x)$ is to use Eratosthene's sieve and its improvements (see later). More clever algorithms exist (Lagarias/Miller/Odlyzko, Deléglise/Rivat, Lagarias/Odlyzko).

II. $\mathbb{Z}/N\mathbb{Z}$ and $(\mathbb{Z}/N\mathbb{Z})^*$

Def. $a \equiv b \bmod N \Leftrightarrow N \mid a - b$.
$\mathbb{Z}/N\mathbb{Z}$ is a quotient ring; representatives of $\equiv$ are generally chosen as $\{0, 1, \ldots, N-1\}$.

Prop.

1. $a \equiv b \bmod N$ and $c \equiv d \bmod N \Rightarrow$

$$a + c \equiv b + d \bmod N, \quad ac \equiv bd \bmod N;$$

2. if $d \mid a, b, N$ then

$$a \equiv b \bmod N \Leftrightarrow a/d \equiv b/d \bmod N/d.$$

Ex. $7^2 \bmod 10 \equiv 49 \bmod 10 \equiv 9 \bmod 10$, $7^3 \equiv 7 \times 9 \equiv 63 \equiv 3 \bmod 10$, $7^4 \equiv 7 \times 3 \equiv 1 \bmod 10$.

Invertible elements

Prop. Invertible elements in $\mathbb{Z}/N\mathbb{Z}$ form the group

$$(\mathbb{Z}/N\mathbb{Z})^* = \{a \in \mathbb{Z}/N\mathbb{Z}, \gcd(a, N) = 1\}.$$

Proof:

Coro. $\mathbb{Z}/N\mathbb{Z}$ is a field iff N is prime.

Def. Euler totient function: $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^*$.

Prop. $\varphi(p^e) = p^e - p^{e-1}$.
Proof:

Prop. $\sum_{d \mid N} \varphi(d) = N$.
Proof:

Order

Def. $\mathrm{ord}_N(a) = \min\{k > 0, a^k \equiv 1 \bmod N\}$.

Prop. Let $t = \mathrm{ord}_N(a)$. Then $a^z \equiv 1 \bmod N \Leftrightarrow t \mid z$.
Proof:

Prop. Let $a \in (\mathbb{Z}/N\mathbb{Z})^*$ and $t = \mathrm{ord}_N(a)$. Then

$$\mathrm{ord}_N(a^i) = t/\gcd(i, t).$$

Proof:

Prop. a) $\mathrm{ord}_N(ab) \mid \mathrm{lcm}(\mathrm{ord}_N(a), \mathrm{ord}_N(b))$.
b) If the orders are prime together, we have an equality.
Proof:

Rem. Take $N = 19$: $\mathrm{ord}_N(7) = 3$, $\mathrm{ord}_N(7^2) = 3$, but $\mathrm{ord}_N(7^3) = 1$.

Lagrange, Fermat, Euler

Thm.(Lagrange) Let G be a finite groupe and $a \in G$. Then $\mathrm{ord}_G(a) \mid \mathrm{Card}(G)$.

Coro.[Fermat's little theorem] Let p be prime and a prime to p. Then

$$a^{p-1} \equiv 1 \bmod p.$$

Coro.[Euler] Let N be an integer and a prime to N. Then

$$a^{\varphi(N)} \equiv 1 \bmod N.$$

Prop. $\mathrm{ord}_N(a) = t = \prod_{i=1}^{r} q_i^{e_i}$ iff $a^t \equiv 1 \bmod N$ and for all i, $a^{t/q_i} \not\equiv 1 \bmod N$.
Proof:

Structure of $(\mathbb{Z}/p\mathbb{Z})^*$

Thm. When p is prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic: there exists g s.t. $\{1, 2, \ldots, p-1\} = \{g^i \bmod p, 1 \leq i \leq p-1\}$.

Lem. For all $d \geq 1$, the number of elements of order d is $\leq \varphi(d)$.
Proof:

Proof of the thm

Rem. a) When $d \mid p-1$, there are exactly $\varphi(d)$ elements of order d.
b) In particular, if g has order $p-1$, the other generators are g^i for $\gcd(i, p-1) = 1$.

Rem. finding a generator is not deterministic polytime, but easily probabilistic.

Structure of $(\mathbb{Z}/p^e\mathbb{Z})^*$

Prop. For all odd p and $e \geq 1$, $(\mathbb{Z}/p^e\mathbb{Z})^*$ is cyclic. Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. If $g^{p-1} \not\equiv 1 \bmod p^2$, then g is a generator of $(\mathbb{Z}/p^e\mathbb{Z})^*$. Otherwise, take $g + p$.
Proof:
Lem. Let $k \not\equiv 0 \bmod p$ ($\neq 2$) and $s \geq 0$. Then

$$(1 + kp)^{p^s} = 1 + k_s p^{s+1},$$

with $p \nmid k_s$.
Proof

Proof

Rem. The only p's for which $2^{p-1} \equiv 1 \bmod p^2$ for $p \leq 1.25 \times 10^{15}$ are 1093 and $p = 3511$.

The case $p = 2$

Prop. $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* = \{1, 3\} = \langle -1 \rangle$. If $e \geq 3$, $(\mathbb{Z}/2^e\mathbb{Z})^* \simeq \langle 5 \rangle \times \langle -1 \rangle$, with $\mathrm{ord}(5) = 2^{e-2}$. Equivalently, all $x \in (\mathbb{Z}/2^e\mathbb{Z})^*$ s'can be written uniquely as

$$x \equiv (-1)^{u(x)} 5^{v(x)} \bmod 2^e$$

with $u(x) \in \{0, 1\}$ and $1 \leq v(x) \leq 2^{e-2}$. Moreover, $u(x) \equiv (x-1)/2 \bmod 2$.
Proof:

Lem. $5^{2^t} = 1 + h_t 2^{t+2}$, with h_t odd.
Proof:

Structure of $(\mathbb{Z}/N\mathbb{Z})^*$

Thm. (Chinese remaindering theorem)

$$\mathbb{Z}/N\mathbb{Z} \sim \prod_{p^e || N} \mathbb{Z}/p^e\mathbb{Z}$$

Proof:

Coro. Let $m_1, \ldots, m_k$ pairwise primes and let $x_1, \ldots, x_k$ be integers. There exists x s.t.

$$x \equiv x_i \bmod m_i$$

for all i. Moreover, x is unique modulo $M = \prod_{i=1}^k m_i$.

Back to Euler

Prop. If $\gcd(N, M) = 1$, then $\varphi(NM) = \varphi(N)\varphi(M)$.
(φ is *multiplicative*).

Lem. x is invertible modulo NM iff x is invertible modulo N and modulo M.

Coro. If

$$N = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

$$\varphi(N) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = N \prod_{i=1}^k (1 - 1/p_i).$$

Fundamental theorem

Thm. $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic iff $N = 2, 4, p^\alpha, 2p^\alpha$, p an odd prime and $\alpha \geq 1$.

Def. (Exponent) $\mathrm{Exp}(G) = \{k, \forall\, a \in G, a^k = 1\}$.

Prop. $\mathrm{Exp}(G) = \mathrm{lcm}\{\mathrm{ord}_G(a), a \in G\}$.

Prop. $\mathrm{Exp}(G_1 \times G_2 \times \cdots \times G_n) = \mathrm{lcm}(\mathrm{Exp}(G_1), \mathrm{Exp}(G_2), \ldots, \mathrm{Exp}(G_n))$.

Carmichael function

Def. (Carmichael function) $\lambda(N) = \mathrm{Exp}((\mathbb{Z}/N\mathbb{Z})^*)$.

Prop.
a) For all $a \in (\mathbb{Z}/N\mathbb{Z})^*$: $a^{\lambda(N)} \equiv 1 \bmod N$.
b) $a^t \equiv 1 \bmod N$ for all a prime to N iff $\lambda(N) \mid t$.

Prop.

(i)	$\lambda(p^e) = \varphi(p^e)$	if p is odd and $e \geq 1$
(ii)	$\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^e) = 2^{e-2}$	if $e \geq 3$
(iii)	$\lambda(\prod_i p_i^{\alpha_i}) = \mathrm{lcm}(\lambda(p_i^{\alpha_i}))$	

Justification of RSA

Prop. If N is squarefree, then for all $a \in \mathbb{Z}$, $a^{\lambda(N)+1} \equiv a \bmod N$.
Proof:

Coro. RSA is valid: for all x, $x^{ed} \equiv x \bmod N$.
Proof:

III. Quadratic reciprocity

Legendre symbol: for prime odd p and $a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } \exists\, x \text{ s.t. } a \equiv x^2 \bmod p \\ -1 & \text{otherwise.} \end{cases}$$

Easy properties:
(i) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$;
(ii) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
(iii) $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$;
(iv) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

Not so easy properties: (Gauss)
(v) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$;
(vi) (Quadratic reciprocity law) p and q odd primes:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Jacobi symbol: $n \in \mathbb{Z}$, $m = \prod_{i=1}^{k} p_i \in \mathbb{Z}$ odd,

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{k} \left(\frac{n}{p_i}\right).$$

Properties: same as for the Legendre symbol.

Ex. Show that $\left(\frac{n}{m}\right) = 0$ iff $\gcd(n, m) > 1$.

IV. Finite fields

Thm. (characteristic) Let $\mathbb{F}$ be a finite field. There exists a smallest $p > 1$ s.t. $p.1_{\mathbb{F}} = 0$; p is prime. The set $\{k.1_{\mathbb{F}}, 0 \leq k < p\}$ is the smallest subfield of $\mathbb{F}$; it is isomorphic to $\mathbb{F}_p$ (prime subfield of $\mathbb{F}$).

Thm.

$$\begin{array}{ccc} \mathbb{F} \times \mathbb{F} & \rightarrow & \mathbb{F} \\ (x, y) & \mapsto & x + y \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbb{F}_p \times \mathbb{F} & \rightarrow & \mathbb{F} \\ (a, x) & \mapsto & ax \end{array}$$

turn $\mathbb{F}$ into a $\mathbb{F}_p$-vector space. If n is the dimension of this space, $\mathbb{F}$ has p^n elements.

Thm. $\mathbb{F}^\times$ is cyclic.

Frobenius

Thm. σ_F :

$$\begin{array}{ccc} \mathbb{F} & \rightarrow & \mathbb{F} \\ x & \mapsto & x^p. \end{array}$$

It is a field automorphism, i.e.

$$\sigma_F(1) = 1, \quad \sigma_F(x + y) = \sigma_F(x) + \sigma_F(y), \quad \sigma_F(xy) = \sigma_F(x)\sigma_F(y).$$

Fixed points are the elements of $\mathbb{F}_p$.
Proof:

Properties of $\mathbf{K}[X]$

Properties close to that of $\mathbb{Z}$, we do not give proofs.
Thm. for all A, B in$\mathbf{K}[X]$, $B \neq 0$. there exists a unique pair (Q, R) in $\mathbf{K}[X]$ s.t.

$$A = BQ + R, \quad \text{with} \quad R = 0 \text{ or } \deg(R) < \deg(B).$$

Thm. (Bézout) There exists U and V in $\mathbf{K}[X]$ s.t.

$$AU + BV = \gcd(A, B).$$

Def. $A(X)$ is irreducible if its degree is ≥ 1, and all its divisors are constant, or $aA(X)$ with $a \in \mathbf{K}^*$.
Thm. We may factor polynomials

$$P = a \prod_{i=1}^{r} P_i^{\alpha_i},$$

where $a \in \mathbf{K}$, P_i monic irreducible and $\alpha_i \in \mathbb{N}$.

Quotient ring

Def. $A \equiv B \pmod f$ iff $A - B$ is a multiple of f.

Def. $\mathbf{K}[X]/f\mathbf{K}[X]$ or $\mathbf{K}[X]/(f)$

Let $\overline{P}$ be the class of P. $\mathbf{K}[X]/(f)$ together with
$\overline{A} + \overline{B} = \overline{A + B}, \quad \overline{A}\,\overline{B} = \overline{AB}$, is a ring.
Canonical representant: for all P, there is a unique R of degree $n - 1$ s.t. $P \equiv R \bmod f$.

With

$$\lambda \cdot \overline{A} = \overline{\lambda A},$$

$\mathbf{K}[X]/(f)$ is $\mathbf{K}$-vector space of dimenstion n. The set $\{\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}\}$ is a basis for this vector space.

Thm. A is invertible modulo f iff $\gcd(A, f) = 1$.

Coro. $\mathbf{K}[X]/(f)$ is a field iff f is irreducible. Moreover, if $\mathbf{K} = \mathbb{F}_p$, $\mathbb{F}_p[X]/(f)$ is a field of cardinality $p^{\deg(f)}$.

More properties

Thm. [CRT] Let $A_1, A_2, \ldots, A_r$ in $\mathbf{K}[X]$ and $Q_1, Q_2, \ldots, Q_r$ polynomials that are pairwise prime. There exists $A \in \mathbf{K}[X]$ s.t.

$$\begin{cases} P \equiv A_1 \pmod{Q_1} \\ P \equiv A_2 \pmod{Q_2} \\ \quad \vdots \\ P \equiv A_r \pmod{Q_r} \end{cases}$$

is equivalent to

$$P \equiv A \pmod{Q_1 Q_2 \ldots Q_r}.$$

$$\mathbf{K}[X]/(Q_1 Q_2 \cdots Q_r) \simeq \mathbf{K}[X]/(Q_1) \times \mathbf{K}[X]/(Q_2) \times \cdots \mathbf{K}[X]/(Q_r).$$

Building finite fields

Thm. (the canonical way) Let $f(X)$ be an irreducible polynomial of degree n over $\mathbb{F}_p$. Then $\mathbb{F}_p[X]/(f(X))$ is a finite field of degree n and cardinality p^n, noted $\mathbb{F}_{p^n}$.

Example

Build $\mathbb{F}_{41^2}$, using a quadratic non-residue modulo 41.

$$\begin{aligned} \left(\frac{7}{41}\right) &= (-1)^{(41-1)/2\times(7-1)/2}\left(\frac{41}{7}\right) \\ &= \left(\frac{41}{7}\right) = \left(\frac{41 \bmod 7}{7}\right) \\ &= \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = \left(\frac{3}{7}\right) = (-1)\left(\frac{7}{3}\right) \\ &= -\left(\frac{1}{3}\right) = -1 \end{aligned}$$

$\Rightarrow \mathbf{K}_1 = \mathbb{F}_{41^2} \sim \mathbb{F}_{41}[X]/(X^2 - 7)$.
This is a vector space of dimension 2 over $\mathbb{F}_{41}$.
Let $\theta = \overline{X}$. All elements can be written $a + b\theta$ where a, b are in $\mathbb{F}_{41}$.
$\theta^2 - 7 = \overline{X^2 - 7} = 0$. We get

$$\theta^2 = 7, \theta^3 = 7\theta, \theta^4 = 8, \ldots, \theta^{80} = 1,$$

so that θ does not generate $\mathbf{K}^*$. The number $\theta + 10$ is found to be a generator.

One application (1/2)

Pb. Given $\left(\frac{a}{p}\right) = 1$, compute $\sqrt{a} \bmod p$.

Case $p \equiv 3 \bmod 4$**:** $r = a^{(p+1)/4} \bmod p$.

Case $p \equiv 1 \bmod 4$**:** find b s.t. $\Delta = b^2 - 4a$ is not a square.

$$\alpha = (-b + \sqrt{\Delta})/2 \quad \Rightarrow \alpha^p = (-b - \sqrt{\Delta})/2 \quad \Rightarrow \alpha\alpha^p = a$$

since $\sqrt{\Delta}^p = \left(\frac{\Delta}{p}\right)\sqrt{\Delta}$.
Let $\beta = \alpha^{(p+1)/2} \bmod (p, X^2 + bX + a)$. Then

$$\beta^2 = \alpha^{p+1} = a.$$

Moreover

$$\beta^p = \beta(\beta^2)^{(p-1)/2} = \beta a^{(p-1)/2} = \beta$$

and β is in $(\mathbb{Z}/p\mathbb{Z})^*$.

One application (2/2)

Let $a = 2 \bmod 41$, which a square; $b = 1$ is s.t. $\Delta = 1 - 4 \times 2 = -7$ which is not a square; hence $\mathbb{F}_{41^2} \sim \mathbb{F}_{41}[X]/(X^2 + X + 2)$.

$$\alpha = X, \quad \alpha^p = 40X + 40, \quad \alpha\alpha^p = 2.$$

$$\beta = X^{(p+1)/2} = 17, \quad 17^2 \equiv 2 \bmod 41.$$

Further properties

Thm. Let $\mathbb{F}$ be a finite field of cardinality q.

$$X^q - X = \prod_{a \in \mathbb{F}} (X - a).$$

Thm.

$$X^{p^n} - X = \prod_{d|n} \prod_{\substack{\deg g = d \\ g \text{ monic irreducible}}} g$$

Thm. The number $I_{n,p}$ of irreducible polynomials of degree n over $\mathbb{F}_p$ is always > 0 and

$$I_{n,p} \approx \frac{p^n}{n}.$$

Thm. For all p and $n \geq 1$, there exists a finite field of cardinality p^n. Two finite fields of the same cardinality are isomorphic.

V. Implementation issues

A) implementing $\mathbb{Z}$

How to code an integer: a positive integer a is stored as an array containing its digits in base $B = 2^\beta$, $\beta = 32, 64$:

$$a = a_{n-1}a_{n-2}\ldots a_0 = \sum_{i=0}^{n-1} a_i B^i.$$

The digits are recovered using successive euclidean divisions of a by B.

Operations:

- $\pm$: idem base 10.
- $\times$: base 10, Karatsuba, FFT $\rightarrow \mathsf{M}(n)$; best is $\tilde{O}(n)$.
- $/$: idem base 10 (?); Newton, $O(\mathsf{M}(n))$.

Multiplication (1/2)

School boy method:

$$A(X) = a_0 + a_1 X, B(X) = b_0 + b_1 X$$
$$P(X) = p_0 + p_1 X + p_2 X^2$$
$$p_0 = a_0 b_0, \quad p_1 = a_0 b_1 + a_1 b_0, \quad p_2 = a_1 b_1$$

Cost: 4 multiplications.
$\Rightarrow O(lm)$ operations.

Karatsuba:

$$p_0 = a_0 b_0, \quad p_2 = a_1 b_1$$
$$p_1 = (a_0 + a_1)(b_0 + b_1) - p_0 - p_2.$$

Cost: 3 multiplications, 2 additions, 2 subtractions.

Multiplication (2/2)

$$n = 2^t$$
$$A(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} = A_0(X) + X^{n/2} A_1(X),$$
$$B(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1} = B_0(X) + X^{n/2} B_1(X),$$
$$\deg(A_i) = \deg(B_i) = n/2 - 1$$

$$P_0 = A_0 B_0, \quad P_1 = (A_0 + A_1)(B_0 + B_1), \quad P_\infty = A_1 B_1$$
$$P(X) = P_0 + X^{n/2}(P_1 - P_0 - P_\infty) + X^n P_\infty.$$

Analysis:

$$M(n) = 3M(n/2)$$

$$M(n) = O(n^{\log_2 3}) = O(n^{1.585})$$

Rem. take care to memory management; branch in naive method for small operands.

Even better: FFT in $O(n^{1+\varepsilon})$.

Gcd algorithms

Overview: classical; binary; Brent; Lehmer; Jebelean, etc. Best is $O(\mathsf{M}(n) \log n)$.

a) Classical Gcd:

```
function gcd(a, b) (* return gcd of a and b *)
1. while b <> 0 do
     r:=a mod b;
     a:=b;
     b:=r;
   endwhile;
2. return a.
3. end.
```


b) binary algorithm: $\gcd(a, b) = \gcd(a, a - b)$ and when b is odd:

$$\gcd(2^k a, b) = \gcd(a, b)$$

Example:

```
a=01111011110
b=01001101000
a=00111101111
b=00001001101
t=00011010001
a=00011010001
b=00001001101
t=00000100001
a=00000100001
b=00001001101
t=00000001011
a=00000100001
b=00000001011
t=00000001011
a=00000001011
b=00000001011
t=00000000000
```


B) $\mathbb{Z}/N\mathbb{Z}$

On top of $\mathbb{Z}$, reduce all operands; Montgomery arithmetic is division free.

- $\mathbb{Z}/p\mathbb{Z}$: choice between a global p and a p per element.
- $\mathbb{Z}/N\mathbb{Z}$: use exceptions to catch divisors of composite N (lazy computations).

Finite fields $\mathbb{F}_{p^n}$

General principle: choose an irreducible polynomial f of degree n over $\mathbb{F}_p$.
Apart from some families and particular cases (e. g., binomials), this is not known to be doable in deterministic polynomial time.
Identify elements of $\mathbb{F}_{p^n}$ to elements of $\mathbb{F}_p^n$ via

$$\overline{a_0 + a_1 X + \cdots + a_{n-1}X^{n-1}} \mapsto (a_0, a_1, \ldots, a_{n-1}).$$

Addition, subtraction are easy; multiplication of polynomials over $\mathbb{F}_p$; inverse via the extended euclidean algorithm.

Rem. When $\mathbb{F}_q$ is small, fix a generator g and represent elements via g^i.

Rem. Composite extensions are not that easy to deal with.

Computing a^e: binary methods

Pb: compute a^e (in any ring).

$$e = 2e' + \varepsilon, \varepsilon \in \{0, 1\}$$

$$a^e = (a^2)^{e'} a^\varepsilon$$

or

$$a^e = (a^{e'})^2 a^\varepsilon.$$

$$a^{11} = (a^2)^5 a = (((a^2)^2)^2 \times a^2)^2 a$$

$$a^{11} = (a^5)^2 a = ((a^2)^2 a)^2 a.$$

Cost: 5 operations (multiplications) to evaluate a^{11}, instead of 10.

The left-right binary method

$$e = e_t 2^t + e_{t-1} 2^{t-1} + \cdots + e_0, e_t = 1$$

Horner: $e = ((\cdots(e_t 2 + e_{t-1})2 + e_{t-2})\cdots)2 + e_0$.

$$a^e = a^{((\cdots(e_t 2 + e_{t-1})2 + e_{t-2}\cdots)2 + e_0} = (((\cdots(a^{e_t})^2 a^{e_{t-1}})^2 a^{e_{t-2}})\cdots)^2 a^{e_0}.$$

```
function ModExp3(a, N, te, nbits)
(* compute de a^e mod N with bits of e *)
(* in te[0..nbits] *)
1. [initialization] b:=a;
2. for i:=nbits-1 .. 0 do
      b:=(b*b) mod N;
      if te[i] = 1 then b:=(b*a) mod N; endif;
   endfor;
3. return b;
4. end.
```


Analysis

$\nu(e)$ number of nonzero bits of e, $\lambda(e) = \lfloor \log(e)/\log 2 \rfloor$

$$C(e) = \lambda(e) T_\square + (\nu(e) - 1) T_{\times a}.$$

On average:

$$\overline{C}(e) = \lambda(e)(T_\square + T_{\times a}/2).$$

If $T_\square = T_{\times a}$, the mean cost of the algorithm is $3/2 \log_2(e) T_{\times a}$.
If a is small, the cost of $T_{\times a}$ is negligeable.

Real life

- Always a good thing to try to implement its own bignum library;
- however, very difficult to be better than GMP, in particular $O(\mathsf{M}(n))$ methods are implemented and very efficient;
- available in any mathematical system (MAPLE, MAGMA, etc.; `pari-gp`, `Sage`, etc.).