MPRI – Cours 2.12.2

F. Morain

Lecture VI: continued fractions and applications

2010/10/12

The slides are available on http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI/2010

I. Motivations

- Approximate π by rationals.
- Solve $1009 = u^2 + v^2$.
- Break some RSA parameters.
- Factor integers (CFRAC, see EThomé's part).

Good reading: Hardy & Wright, A. M. Rockett and P. Szüsz, etc.

Rem. Pre-dates LLL, and has still some interest.

II. Continued fractions

Lemma. (Dirichlet) Let $\theta \in \mathbb{R}$, $Q \in \mathbb{N}$: $\exists\,(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ s.t.

$$\left|\frac{p}{q} - \theta\right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}.$$

Proof: spread the $\{n\theta\}$ for $0 \leq n \leq Q$ in $[0, 1/Q[, \ldots, [(Q-1)/Q, 1]$.
Pigeon hole principle (*principe des tiroirs de Dirichlet*): $\exists\, i, h, k < h$ s.t. $\{h\theta\}, \{k\theta\} \in [i/Q, (i+1)/Q[$.
Let $q = h - k$

$$q \leq Q \text{ and } \{q\theta\} \leq 1/Q$$

$$q\theta = \lfloor q\theta \rfloor + \{q\theta\} = p + \{q\theta\}$$

$$|p - q\theta| \leq 1/Q$$

$$\left|\frac{p}{q} - \theta\right| \leq \frac{1}{qQ}. \quad \Box$$

Approximating reals numbers by rationals (1/2)

Coro. If $\theta \notin \mathbb{Q}$, $\exists$ an infinity of p/q s.t.

$$\left|\frac{p}{q} - \theta\right| \leq \frac{1}{q^2}.$$

Proof: If $\theta = a/b \in \mathbb{Q}$: $(b > 0)$

$$\left|\frac{a}{b} - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

($q > 0$ and $a/b \neq p/q$) implies

$$\frac{1}{bq} \leq \frac{1}{q^2} \Leftrightarrow q \leq b.$$

Approximating reals numbers by rationals (2/2)

If $\theta \notin \mathbb{Q}$: let $p_1/q_1, p_2/q_2, \ldots, p_s/q_s$ all the rational numbers s.t.

$$\forall i, \left|\theta - \frac{p_i}{q_i}\right| \leq \frac{1}{q_i^2}$$

$$\varepsilon = \min_{1 \leq i \leq s} \left|\theta - \frac{p_i}{q_i}\right| > 0.$$

Let Q be an integer $> 1/\varepsilon$.
Dirichlet $\Rightarrow \exists p, q$ s.t.

$$\left|\theta - \frac{p}{q}\right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}.$$

$$\frac{1}{qQ} < \frac{\varepsilon}{q} \leq \varepsilon. \qquad \Box$$

Finite continued fractions

$$[a_0, \ldots, a_N] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cdots + \cfrac{1}{a_{N-1} + \cfrac{1}{a_N}}}}.$$

a_i i-th partial quotient (*i-ième quotient partiel*).

$$\forall M \geq 0, [a_0, a_1, \ldots, a_M, [a_{M+1}, \ldots, a_N]] = [a_0, a_1, \ldots, a_N]$$

$$p_{-2} = 0, p_{-1} = 1, q_{-1} = 0, q_{-2} = 1$$

$$p_n = a_n p_{n-1} + p_{n-2},$$

$$q_n = a_n q_{n-1} + q_{n-2}.$$

Prop. $\forall n \leq N, [a_0, \ldots, a_n] = \frac{p_n}{q_n}$

p_n/q_n n-th convergent (*n-ième convergent ou réduite*) of the continued fraction.

Properties of convergents

Prop.

$$\forall n, p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}.$$

Coro. If $a_i > 0$, $p_i, q_i \geq 0$ and strictly increasing s.t.

$$\forall n, [a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n} = a_0 + \frac{1}{q_1 q_0} - \frac{1}{q_2 q_1} + \cdots + \frac{(-1)^{n-1}}{q_n q_{n-1}}.$$

Prop. For all $n \geq 1$:

$$p_n q_{n-2} - p_{n-2} q_n = (-1)^{n-1} a_n.$$

Coro. p_{2n}/q_{2n} is increasing, p_{2n+1}/q_{2n+1} is decreasing. Moreover, for all n

$$\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}}.$$

III. Continued fractions with integer coefficients

Prop. For all n, $q_n \geq n$ and for all $n \geq 2$, $q_n \geq q_{n-1} + 1$.

Prop. p_n and q_n are prime together.

Prop. If $x \in \mathbb{Q}^+$, there are two continued fractions representing x.
Proof: let $x = [a_0, a_1, \ldots, a_N]$. If $a_N \geq 2$, then

$$x = [a_0, a_1, \ldots, a_N - 1, 1]$$

(with $N + 1$ terms). If $a_N = 1$:

$$x = [a_0, a_1, \ldots, a_{N-1} + 1]$$

(with $N - 1$ terms). $\Box$

Complete quotients

Def. $a'_n = [a_n, a_{n+1}, \ldots, a_N]$, n-th complete quotient (n-*ième quotient complet*).
Prop. $[a_0, \ldots, a_N] = [a_0, \ldots, a_{n-1}, a'_n]$.
Prop. Consider $[a_0, a_1, \ldots, a_N]$. For all $0 \le n \le N$, we have $a_n = \lfloor a'_n \rfloor$ except when $a_N = 1$, in which case $a_{N-1} = \lfloor a'_{N-1} \rfloor - 1$.
Proof: Let $a'_n = [a_n, \ldots, a_N]$. If $n = N$, $a'_n = a_N$. If $n = N-1$:

$$a'_n = a_n + \frac{1}{a_N}.$$

If $a_N = 1$, we have $a_N = \lfloor a'_n \rfloor - 1$ and if $a_N \ge 2$, we have $a_n = \lfloor a'_n \rfloor$.
If $n \le N-2$:

$$a'_n = [a_n, a'_{n+1}] = a_n + \frac{1}{a'_{n+1}}$$

with $a'_{n+1} > 1$, hence $a_n = \lfloor a'_n \rfloor$. $\square$

Unicity of the expansion (1/2)

Thm. Let $[a_0, a_1, \ldots, a_N] = [b_0, b_1, \ldots, b_M] = x$ with $a_i, b_j > 0$, $a_N \ge 2$, $b_M \ge 2$. Then $N = M$ and $a_i = b_i$ for all i.

Proof: assume $N \le M$; we use induction and prove $a_i = b_i$ for all i. For all n, $a_n = \lfloor a'_n \rfloor$, $b_n = \lfloor b'_n \rfloor$ (since $a_N \ge 2$, $b_M \ge 2$). In particular $x = a'_0 = b'_0 \Rightarrow a_0 = b_0$.

Hyp. $a_i = b_i$ pour $i \le n-1 < N$
Write

$$x = \frac{a'_n p_{n-1} + p_{n-2}}{a'_n q_{n-1} + q_{n-2}} = \frac{b'_n p_{n-1} + p_{n-2}}{b'_n q_{n-1} + q_{n-2}}$$

with $p_{n-1}, p_{n-2}, q_{n-1}, q_{n-2}$ only depending on $(a_i = b_i)$ for $0 \le i \le n-1$.

Unicity of the expansion (2/2)

Reorganizing things

$$(a'_n p_{n-1} + p_{n-2})(b'_n q_{n-1} + q_{n-2}) = (b'_n p_{n-1} + p_{n-2})(a'_n q_{n-1} + q_{n-2})$$

or

$$a'_n(p_{n-1}q_{n-2} - q_{n-1}p_{n-2}) - b'_n(p_{n-1}q_{n-2} - q_{n-1}p_{n-2}) = 0,$$

or $a'_n = b'_n$, or $a_n = b_n$.

If $M > N$:

$$x = \frac{p_N}{q_N} = \frac{b'_{N+1}p_N + p_{N-1}}{b'_{N+1}q_N + q_{N-1}}$$

hence $p_N q_{N-1} = p_{N-1} q_N$. $\square$

Expansion of a rational number

Thm. Let $x = h/k \in \mathbb{Q}^+$, $(h,k) = 1$; we can expand x as $[a_0, \ldots, a_N]$ where (a_i) is given by the Euclidean algorithm applied on (h,k).
Proof:

$$\begin{array}{rcl} h & = & a_0 k + k_1, 0 \le k_1 < k, \\ k & = & a_1 k_1 + k_2, \\ & \ldots & \\ k_{i-1} & = & a_i k_i + k_{i+1}, 0 \le k_{i+1} < k_i, \\ & \ldots & \\ k_{N-2} & = & a_{N-1} k_{N-1} + k_N, \\ k_{N-1} & = & a_N k_N, \end{array}$$

and $k_{N+1} = 0$. Since $(h,k) = 1$, $k_N = 1$ and $k_{N-1} \ge 2$, which implies $a_N \ge 2$.

$$\forall\, i, \frac{k_{i-1}}{k_i} = a'_i = [a_i, \ldots, a_N].\square$$

Rem. $h/k = p_N/q_N$; $hq_{N-1} - kp_{N-1} = 1$

Continued fraction expansion of a real number (1/3)

$$a_0 = \lfloor x \rfloor,$$
$$x = a_0 + x_1, 0 \leq x_1 < 1,$$
$$\frac{1}{x_1} = a_1' = a_1 + x_2, 0 \leq x_2 < 1.$$

If $x_i \neq 0$, then x_{i+1} is defined by

$$\frac{1}{x_i} = a_i' = a_i + x_{i+1}, 0 \leq x_{i+1} < 1.$$

When $x \in \mathbb{Q}$, the algorithm terminates since $x_i = k_{i+1}/k_i$ and (k_i) decreases. If $x \notin \mathbb{Q}$, $x_i \notin \mathbb{Q}$ and the algorithm does not terminate.

Define (p_n) and (q_n) as usual and introduce $q_n' = a_n' q_{n-1} + q_{n-2}$.

Continued fraction expansion of a real number (2/3)

Prop. For all n

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n+1}'}.$$

Coro. Let $x \in \mathbb{R} - \mathbb{Q}, x > 0$. For all $n \geq 0$

$$\frac{p_{2n}}{q_{2n}} \leq x < \frac{p_{2n+1}}{q_{2n+1}}.$$

Rem. The two sequences (p_{2n}/q_{2n}) et (p_{2n+1}/q_{2n+1}) are adjacent, since

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n}q_{2n+1}} \leq \frac{1}{2n(2n+1)}.$$

These two sequences define x.

Continued fraction expansion of a real number (3/3)

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, \ldots]$$
$$\pi - \frac{22}{7} \approx -0.00126, \quad \pi - \frac{355}{113} \approx -0.2667 \times 10^{-6}.$$

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, \ldots]$$

Thm. The probability that $a_n = a$ is approximately

$$p(a) = \frac{\log(1 + 1/a) - \log(1 + 1/(a+1))}{\log 2}.$$

a	$p(a)$
1	0.415
2	0.170
3	0.093
4	0.059

IV. Approximating x by p_n/q_n

Thm. For all n

$$\left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}}.$$

Thm. (Best approximation) Let p_n/q_n be a convergent of $x > 0$. Then, for all integer p and all $q < q_n$,

$$|qx - p| > |q_n x - p_n|$$

or equivalently

$$\left| x - \frac{p}{q} \right| > \left| x - \frac{p_n}{q_n} \right|.$$

Approximating (2/3)

Thm. Let p_n/q_n and p_{n+1}/q_{n+1} be two consecutive convergents of $x > 0$. One of them satisfies

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{2q^2}.$$

Proof: remark that $p_n/q_n - x$ and $p_{n+1}/q_{n+1} - x$ are of opposite sign:

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_{n+1}}{q_{n+1}} - x\right| + \left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}.$$

If

$$\left|\frac{p_n}{q_n} - x\right| > \frac{1}{2q_n^2} \text{ and } \left|\frac{p_{n+1}}{q_{n+1}} - x\right| > \frac{1}{2q_{n+1}^2},$$

then

$$\frac{1}{q_n q_{n+1}} > \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} \iff \left(\frac{1}{q_n} - \frac{1}{q_{n+1}}\right)^2 < 0.\square$$

Approximating (3/3)

Thm. One of p_n/q_n, p_{n+1}/q_{n+1}, p_{n+2}/q_{n+2} satisfies

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{\sqrt{5}q^2}.$$

Thm. (Tong) Let $\tau \in \mathbb{R}^+$. One of p_{2n-1}/q_{2n-1}, p_{2n}/q_{2n}, p_{2n+1}/q_{2n+1} satisfies

$$-\frac{\tau}{\sqrt{a_{2n+1}^2 + 4\tau}}\frac{1}{q^2} < x - \frac{p}{q} < \frac{1}{\sqrt{a_{2n+1}^2 + 4\tau}}\frac{1}{q^2}.$$

Converse theorems

Thm. Let p/q s.t.

$$\left|\frac{p}{q} - x\right| \leq \frac{1}{2q^2}.$$

Then p/q is a convergent of the continued fraction expansion of x.

Thm. If

$$\left|\frac{p}{q} - x\right| < \frac{1}{q^2}$$

then p/q is a convergent or a an intermediary one: sitting in between p_{n-1}/q_{n-1} and p_n/q_n are $(p_{n-1} \pm p_n)/(q_{n-1} + q_n)$.

Example: solving the Pell-Fermat equation

Pb. For given $d > 1$, find all integer solutions of

$$x^2 - dy^2 = 1.$$

Since $x > \sqrt{d}\,y$, we get

$$|x - y\sqrt{d}| < \frac{1}{2\sqrt{d}\,y}$$

or

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}$$

$$\Rightarrow \frac{x}{y} \text{ is a convergent of } \sqrt{d}.$$

Thm. All solutions are obtainable via $(x + y\sqrt{d})^n$.

Periodic continued fractions (1/2)

$$[a_0, a_1, \ldots, \overline{a_{n_0}, a_{n_0+1}, \ldots, a_{n_0+T-1}}]$$

Thm. The expansion of x is periodic iff x is a root of some $ax^2+bx+c=0$ with integer coefficients, $b^2-4ac \neq 0$, $a \neq 0$.
Thm. We have $\sqrt{d} = [(a_n)] = [a_0, \overline{a_1, a_2, \ldots, a_n, 2a_0}]$ with

$$u_0 = 0, v_0 = 1,$$

$$\alpha_n = a_n' = [a_n, \ldots] = \frac{u_n + \sqrt{d}}{v_n}, a_n = \lfloor \alpha_n \rfloor,$$

$$u_{n+1} = a_n v_n - u_n, v_{n+1} = \frac{d - u_{n+1}^2}{v_n},$$

$$\frac{p_n}{q_n} = [a_0, \ldots, a_n],$$

$$p_{n-1}^2 - dq_{n-1}^2 = (-1)^n v_n, |v_n| \leq 2\sqrt{d}, p_{-2} = 0, p_{-1} = 1$$

Periodic continued fractions (2/2)

Rem. Direct application to Pell-Fermat (and/or finding units in real quadratic fields).

Ex. $\sqrt{a^2+1} = [a, \overline{2a}]$.

Conj. $n \ll \sqrt{d}\log\log d$ for $d \equiv 1 \bmod 8$ and $\sqrt{d}\log\log(4d)$ otherwise.

V. Applications

A) Solving $p = x^2 + y^2$

Thm. Let p be prime. Then $p = x^2 + y^2$ iff $p = 2$ or $p \equiv 1 \bmod 4$.
Application: compute easily $\#E : Y^2 = X^3 + X$ over $\mathbb{F}_p$, which is $p + 1 \pm 2x$ or $p + 1 \pm 2y$ (this can be given exactly).

Necessary condition: $(x/y) \equiv -1 \bmod p$ has a solution iff $p \equiv 1 \bmod 4$.

Algorithm: solve $a^2 + 1 \equiv 0 \bmod p$; x/y will be some convergent of a/p.

Rem. Can be generalized to $x^2 + dy^2 = p$ (Cornacchia's algorithm).

Cont'd

Prop. Let $n \geq 2$, $a \geq 1$ and $n \mid a^2 + 1$: $\exists (s,t)$ s.t. $n = s^2 + t^2$.

Proof: write $a/n = [a_0, a_1, \ldots, a_N]$. Choose $s = q_k$ s.t. $q_k \leq \sqrt{n} < q_{k+1}$.
If $q_1 = a_1 = 1$ and $q_2 > \sqrt{n}$, put $k = 1$ and $s = q_1 = 1$.
a/n is in between of p_k/q_k and p_{k+1}/q_{k+1}:

$$\left|\frac{a}{n} - \frac{p_k}{q_k}\right| \leq \left|\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right| = \frac{1}{q_k q_{k+1}} < \frac{1}{\sqrt{n} q_k}.$$

Let $t = |aq_k - np_k|$: $t^2 < n$, $1 \leq s^2 \leq n \Rightarrow 1 \leq s^2 + t^2 \leq 2n - 1$.

But $s^2 + t^2 = q_k^2 + (aq_k - np_k)^2 \equiv q_k^2(1 + a^2) \equiv 0 \bmod n$. The only possible multiple is n and $s^2 + t^2 = n$. $\square$

B) RSA with small exponent (Wiener)

$$N = pq, ed \equiv 1 \bmod \varphi(N)$$

Rem. Given $\varphi(N) = (p-1)(q-1)$, we can get $p+q$, from which we get p and q using a degree 2 equation.
Prop. for all N, $N - 3\sqrt{N} < \varphi(N) < N$.
Thm. If $p < q < 2p$, $e < N$ et $d < \sqrt[4]{N}/3$, we can recover the factorization of N.
Proof: $\exists k$, $ed - k\varphi(N) = 1$; one finds

$$\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{3k}{d\sqrt{N}} < \frac{1}{2d^2}.\square$$

Rem. DeWeger02: use $\varphi(N) \approx N + 1 - 2\sqrt{N}$.

Rem. Many improvements by Boneh, Durfee, etc.