On an algorithm for finding fixed point of certain contraction maps and its application to point counting

Takakazu Satoh
Department of Mathematics,
Faculty of Science,
Saitama University

Sheet 2 Cryptographic background

In order to make elliptic curve cryptosystems secure, we need to select a curve which is not vulnerable (at least) to known attacks.

Efficiency of some attacks depends on the order of rational points of the given elliptic curve/$\mathbf{F}_{p^N}$. Elliptic Curve Point Counting(ECPC) is necessary to avoid these attacks.

l-adic method (SEA algorithm): applicable for any p
p-adic method: in practice, only for small p, but it runs faster than SEA for those p.

Sheet 3 Motivation

P. Gaudry's observation (e-mail message, 2001):
SST is applicable to a polynomial which is closely linked to the AGM.

$$E_2(\lambda, \lambda') = \lambda'^2(1+\lambda)^2 - 4\lambda$$

The SST algorithm is not specific to the modular polynomial Φ_p.

Our problem: To which class of function can we apply the technique in SST?

Sheet 4 Outline

- Formulation and interpretation
- Acceleration of convergence
- Implementational remarks
- Applications
  - Teichmüller lift (used in ECPC for $p=3$)
  - Acceleration of AGM for $p=2$.

Sheet 5 Notation

$\mathbf{Q}_p$: the field of p-adic numbers
$\mathbf{Z}_p$: the ring of p-adic integers
K: unramified extension of degree N over $\mathbf{Q}_p$

$|\cdot|$: p-adic valuation on K normalized as $|p| = p^{-1}$.
R: the valuation ring of K.
$R/pR \cong \mathbf{F}_q$ with $q := p^N$.
An element τ of $\mathrm{Gal}(K/\mathbf{Q}_p)$ is an isometry on K.
τ induces $\bar\tau \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$ by $\bar\tau(x) := \overline{\tau(X)}$ where $\overline{X} = x$.

$$\begin{array}{ccc} \mathrm{Gal}(K/\mathbf{Q}_p) & \cong & \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p) \\ \Cup & & \Cup \\ \exists\sigma\colon p\text{-th Frob. subst} & \to & p\text{-th power map} \end{array}$$

Sheet 6 **Representation of R**

Let $F(X) := \sum_{i=0}^{N} a_i X^n \in \mathbf{Z}[X]$ be a monic (low weight) polynomial of degree N such that $0 \le a_i < p$ and that F is irredicible over $\mathbf{Z}_p$ and that $F \bmod p$ is s.q.f.
$R = \mathbf{Z}_p[\theta] \cong \mathbf{Z}_p[X]/\langle F(X)\rangle$ (θ is a class of X in RHS).
ψ: the $(p^N - 1)$-th root of unity satisfying $\psi \equiv \theta \bmod p$.
G: the monic minimal polynomial of ψ over $\mathbf{Z}_p$.
$R = \mathbf{Z}_p[\psi] \cong \mathbf{Z}_p[X]/\langle G(X)\rangle$ (ψ is a class of X in RHS).

Arithmetic operations on R w.r.t. ψ are three times slower than those w.r.t. θ.

We assume an arithmetic operation on $R/p^M R$ ($\cong$ $(\mathbf{Z}/p^M\mathbf{Z})[\psi]$) amounts to $O((MN)^{\mu})$ bit operations.

Sheet 7 **Evaluation of the Frobenius**

With ψ-representation, we can evaluate the Frobenius substitution σ^{-1} with $(p-1)$ multiplications on $\mathbf{Z}_p[X]$ and one reduction mod $G(X)$.

Although $\sigma(x) \ne x^p$ in general, $\sigma(\psi) = \psi^p$.
Thus $\sigma^{-1}(\psi^{mp+i}) = \psi^m \sigma^{-1}(\psi)^i$ and

$$\sigma^{-1}\left(\sum_{n=0}^{N-1} a_n \psi^n\right) = \sum_{i=0}^{p-1} \left(\sum_{0 \le mp+i < N} a_{mp+i}\psi^m\right) b_i \quad (b_i := \sigma^{-1}(\psi^i)).$$

Evaluation of $\sigma^{-1}(x) \bmod p^M$ needs $O((NM)^{\mu})$ bit ops.

With θ-representation, $\sigma^{-1}\left(\sum_{n=0}^{N-1} c_n\theta^n\right) = \sum_{n=0}^{N-1} c_n \sigma^{-1}(\theta)^n$ where $\sigma^{-1}(\theta)$ is precomputed.

Sheet 8 **Assumptions**

$a \in R$, $m \in \mathbf{N}$, $U := a + p^m R$, $f : U \to K$.
Analyticity on U
  (*) $f(x) = \sum_{r=0}^{\infty} f^{(r)}(a)(x-a)^r/r!$ for all $x \in U$.
Coefficient size
  $f^{(r)}(a) \in K$ and $\left|\frac{1}{r!} f^{(r)}(a)\right| \le |p|^{1-m(r-1)}$ for all $r \in \mathbf{N}$. (Rem: This does *not* imply (*))
Initial value
  We have $x_0 \in U$ s.t. $|\sigma^{-1}(f(x_0)) - x_0| \le |p|^m$.

Complexity

$f(x) \bmod p^M$ is evaluated with $O((NM)^{\mu})$ bit op.

Sheet 9 **Consequences**

---

(1) We can define an infinite sequence $\{x_i\}_{i=1}^{\infty}$ by $x_i := \sigma^{-1}(f(x_{i-1}))$.
(Note this also asserts $x_i \in U$.)

(2) $\xi := \lim_{i \to \infty} x_i$ exists and ξ is a unique fixed point of $\sigma^{-1} \circ f$ in U.

(3) $\xi \bmod p^M$ can be obtained with $O(N^{\mu} M^{\mu + 1/(1+\mu)})$ bit operations.

Sheet 10 **Properties on K**

$(K, |\cdot|)$ is a **complete** valuation field.
Moreover, $|\cdot|$ is **non-Archimedean**, i.e.

$$|x+y| \leq \max(|x|, |y|)$$

Using this ultra triangle inequality, we see:

(1) $\{a_n\}_{n=1}^{\infty}$ is the Cauchy seq. $\leftrightarrow$ $\lim_{n \to \infty} |a_n - a_{n+1}| = 0$.

(2) $\sum_{n=1}^{\infty} a_n$ converges $\leftrightarrow$ $\lim_{n \to \infty} a_n = 0$.

(3) For any bijection $s : \mathbf{N} \to \mathbf{N}$, $\sum_{n=1}^{\infty} a_{s(n)} = \sum_{n=1}^{\infty} a_n$.

Rem: All of them are false in $\mathbf{R}$.
An explicit counter example to (3):

$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \log 2, \quad 1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \cdots = \frac{3}{2} \log 2$

Sheet 11 **Fixed points**

Using

$$\left| \frac{1}{r!} f^{(r)}(a) \right| \leq |p|^{1-m(r-1)} \quad \text{for } \forall r \in \mathbf{N},$$

we have

$$\left| \frac{1}{r!} f^{(r)}(x) \right| \leq |p|^{1-m(r-1)} \quad \text{for } \forall r \in \mathbf{N}, \forall x \in U.$$

From this,

$$|f(x') - f(x)| \leq |p| \, |x' - x|.$$

Since $\sigma : K \to K$ is an isometry (w.r.t. $|\cdot|$), existence and uniqueness of a fixed point of $\sigma^{-1} \circ f$ follows from metric space theory. (Actually, the proof is easier since $|\cdot|$ is non-Archimedean.)

Sheet 12 **Fixed points (2)**

The proof essentially uses the analyticity of f.

Cf. There is an injective C^{∞} function $g : K \to K$ s.t. $g'(x) = 0$ identically.
(Dieudonné: Bull. Sci. Math. **68**(1944) 79-85)

Note also σ is *not* differentiable (as a one variable function on K).

Sheet 13 **Naive algorithm**

Recall that $\xi \in U$ is the unique fixed point of $\sigma^{-1} \circ f$.
We can prove that $x_i \equiv \xi \bmod p^{m+i}$.
Input: $M \in \mathbf{N}$, $x_0 \in U$
Output: $\xi \bmod p^M$
Procedure:

1: $x := x_0$;
2: **for** $(i=0 \ ; \ i<M-m \ ; \ ++i)$
3: $\quad x := \sigma^{-1}(f(x)) \bmod p^{m+i+1}$;
4: **return** x ;

The time complexity of the above algorithm is $O(N^{\mu} M^{\mu+1})$ bit operations.

Sheet 14 **improvement**

The naive method evaluates f many times "from scratch".
$|x_{i+1}-x_i| \le |p|^{m+i} \Rightarrow |f(x_{i+1})-f(x_i)| \le |p|^{m+i+1}$
This means that "most part of" $f(x_{i+1})$ is already computed when we obtain $f(x_i)$.

Put $d_i := x_i - x_{i-1}$. Then

$$\begin{aligned} d_{i+1} &= x_{i+1} - x_i = \sigma^{-1}(f(x_i) - f(x_{i-1})) \\ &= \sigma^{-1}\left(f'(x_{i-1})\, d_i + \frac{f^{(2)}(x_{i-1})}{2} d_i^2 + \cdots\right) \\ d_{i+1} &\equiv \sigma^{-1}(f'(x_i))\sigma^{-1}(d_i) \mod p^{2i+m-1} \end{aligned}$$

Sheet 15 **Improvement (2)**

Assume we have computed x_i (hence x_{i-1}, too).

$$x_{i+1} = x_i + d_{i+1} \equiv x_i + \sigma^{-1}(f'(x_i))\sigma^{-1}(d_i) \mod p^{m+i+1} \qquad (*)$$

(for $i \ge 3$).

Since $d_i \equiv 0 \bmod p^{m+i-1}$, the multiplication in (*) is essentially performed in R/pR $(=\mathbf{F}_q)$.

This is much faster than multiplication in R.

Moreover, $p^{-1}f'(x_i) \equiv p^{-1}f'(x_1) \bmod p$ for $i \ge 2$.
No need to compute $\sigma^{-1}(f'(x_i))$ for $i \ge 2$.

Sheet 16 **Improvement (3)**

But if we compute $x_i \bmod p^{m+i}$ by

$$x_i = x_0 + d_1 + d_2 + \cdots d_i,$$

we need $d_0, \ \ldots, \ d_i \bmod p^{m+i}$.
This nullifies complexity saving by performing multiplication in

$$x_{i+1} = x_i + d_{i+1} \equiv x_i + \sigma^{-1}(f'(x_i))\sigma^{-1}(d_i) \mod p^{m+i+1}$$

with $\bmod p$.

This again results in an $O(N^{\mu}M^{\mu+1})$ algorithm.

Sheet 17 **SST acceleration**

(*) $d_{i+1} \equiv \sigma^{-1}(f'(x_i))\sigma^{-1}(d_i) \bmod p^{2i+m-1}$.

Choose $W \in \mathbf{N}$ (determined later).
Output: the fixed point ξ of $\sigma^{-1}\circ f$
Procedure:
1: compute $x_W \bmod p^{W+m}$ and lift it to $R/p^{2W+m}R$
2: $d_{W+1} := \sigma^{-1}(f(x_W)) - x_W \bmod p^{2W+m}$
3: $x_{2W} := x_W + (d_{W+1} + \underbrace{d_{W+2} + \cdots + d_{2W}}_{\text{use}(*),\ \text{essentially} \bmod p^W})$
4: $d_{2W+1} := \sigma^{-1}(f(x_{2W})) - x_{2W} \bmod p^{3W+m}$
5: $x_{3W} := x_{2W} + (d_{2W+1} + \underbrace{d_{2W+2} + \cdots + d_{3W}}_{\text{use}(*),\ \text{essentially} \bmod p^W})$
6: and so on...

Sheet 18 **SST acceleration (2)**

Procedure:
$x := x_W$; // use the naive algorithm
$u := \sigma^{-1}(f'(x)) \bmod p^W$;
for $(i := 1$; $iW < M$; $i := i+1)$ {
  $y := \sigma^{-1}(f(x)) \bmod p^{(i+1)W+m}$;
  $d := (p^{-iW-m}(y-x)) \bmod p^W$; $s := d$;
  for $(j := 1$; $j < W$; $j := j+1)$
    $s := u\sigma^{-1}(s) + d \bmod p^{j+1}$; // Horner's method
  $x := x + p^{iW+m}s \bmod p^{(i+1)W+m}$;
}
return x ; // $\xi \bmod p^{M+m}$

Space complexity: $O(1)$ variables used.

Sheet 19 **Choice of W**

To minimize the growth rate of the time complexity of the resulting algorithm, we determine W so that time to compute d_{mW+1} (out side of the inner loop) and $d_{mW+2} + \cdots + d_{m(W+1)}$ (inner loop) are equal.

Letting $W = M^{\alpha}$, we obtain an equation on α.
Its root is $\alpha = \mu/(\mu+1)$.
The time complexity: $O(N^{\mu}M^{\mu+1/(\mu+1)})$.

This minimizes only growth rate.

The optimal value for W depends on implementation, a platform and f.

Sheet 20 **Choice of W (2)**

For 32 bit CPU, time to multiply two 32 bit unsigned integers is the same as time to multiply two 17 bit unsigned integers.

Assumption: time to perform arithmetic operation on $R \bmod 2^{17}$ and $R \bmod 2^{32}$ is the same.

Actually, this assumption is questionable, (pack-to-integer technique, HW implementation....) but we assume it.

W is chosen to a multiple of w, the CPU word size.
The inner loop is performed modulo $p^{\lceil (j+1)/w \rceil w}$

Sheet 21 **Application**

(1) Teichmüller lift (used in ECPC/fields of odd char.)
Elliptic curves/$\mathbf{F}_{3^n}$ in ECC
- Smart, Westwood: Point multiplication on ordinary elliptic curves over fields of characteristic three, (available at IACR e-print archive)
- Galbraith, Harrison, Soldera: Implementing the Tate pairing, in Proc. ANTS-5 (SLNCS 2369)

(2) AGM point counting ($p=2$)

Sheet 22 **Teichmüller lift**

$a \in \mathbf{F}_q^\times$

The Teichmüller lift $\mathscr{T}(a)$ of a is the unique $(q-1)$-th root of unity s.t. $\mathscr{T}(a) \bmod p = a$.

$\mathscr{T}(a) = \sigma^{-1}(\mathscr{T}(a)^p) \Rightarrow$ We can apply our result to $f(x) = x^p$ with $m=1$ (and $x_0 :=$ any lift of a to $R^\times$.)

The uniqueness of the fixed point implies that the fixed point of $\sigma^{-1} \circ f$ is $\mathscr{T}(a)$.

$$R \underset{\pi}{\overset{\mathscr{T}}{\rightleftarrows}} \mathbf{F}_p \qquad (\pi\text{: mod } p \text{ map})$$

Computation of $\mathscr{T}(a) \bmod p^M$: $O(N^\mu M^{\mu+1/(\mu+1)})$ bit op.

Sheet 23 **Relation to ECPC**

$E/\mathbf{F}_q$: a given ordinal elliptic curve
$V_p^\uparrow : E^\uparrow \to \sigma^{-1}(E^\uparrow)$ the lift of the p-th Verschiebung
$\uparrow$ denotes the canonical lift.
c: leading coefficient of $V_p^\uparrow$
$\mathrm{Tr}(\mathrm{Fr}_p) \equiv N_{K/\mathbf{Q}_p}(c) \bmod p^{N/2+O(1)}$

$$N_{K/\mathbf{Q}_p}(c) = N_{K/\mathbf{Q}_p}(\underbrace{c/\mathscr{T}(\pi(c))}_{\equiv 1 \bmod p})\mathscr{T}(N_{\mathbf{F}_q/\mathbf{F}_p}(\pi(c)))$$

Note $N_{K/\mathbf{Q}_p}\mathscr{T}(a) = \mathscr{T}(N_{\mathbf{F}_q/\mathbf{F}_p} a)$. If p is odd,

$$N_{K/\mathbf{Q}_p}(x) = \exp(\mathrm{Tr}_{K/\mathbf{Q}_p}(\log x)) \text{ for } x \equiv 1 \bmod p$$

and RHS is evaluated with $O(N^{\mu} M^{\mu+1/2})$ bit ops.

Sheet 24 **AGM based ECPC**

AGM ECPC ($p=2$, $q=2^N$): $\Psi(x) := \dfrac{1+x}{2\sqrt{x}}$

Input: $a \in \mathbf{F}_q^{\times}$

Output: $\mathrm{Tr}\,\mathrm{Fr}_q$ on $y^2+xy=x^3+a$

Procedure:

1: $c := 1+8(\text{lift of } a)$; $M := N/2+1$;

2: **for** $(i := 0$; $i < M-1$; $i := i+1)$

3: $\quad c := \Psi(c)$;

4: **return** t s.t. $t \equiv N_{K/\mathbf{Q}_2}\left(\dfrac{2c}{1+c}\right) \bmod 2^M$, $|t| \le 2\sqrt{q}$

($\dfrac{2c}{1+c} \equiv 1 \bmod 8$, so Teichmüller lift is unnecessary.)

Sheet 25 **Acceleration of AGM (1)**

$E : y^2+xy=x^3+a$.

Define:

$c_{0,m} := 1+8\sigma^{-m}(a)$, $c_{n,m} := \Psi(c_{n-1,m})$

$x_0 := 1+8a$, $x_n := \sigma^{-1}(\Psi(x_{n-1}))$

Then: $c_{n,n} = x_n$

i.e. x_n is the n-th value of AGM process for $\sigma^{-n}(E)$.

$\mathrm{Tr}(E) = \mathrm{Tr}(\sigma^{-n}(E))$

We can replace $c := \Psi(c)$ by $c := \sigma^{-1}(\Psi(c))$.

For any $c \in 1+8R^{\times}$, $\sigma^{-1}(\Psi(c)) \equiv c \bmod 16$

Sheet 26 **Acceleration of AGM (2)**

$\Psi(x) = 1+\dfrac{1}{8}(x-1)^2-\dfrac{1}{8}(x-1)^3+\dfrac{15}{128}(x-1)^4+\cdots$

$\left|\dfrac{1}{r!}\Psi^{(r)}(1)\right| \le |2|^{1-2r}$.

$\Psi_2(x) := \Psi(x)-\dfrac{1}{8}(x-1)^2$. Then, $\left|\dfrac{1}{r!}\Psi_2^{(r)}(1)\right| \le |2|^{1-3(r-1)}$.

$\left|\dfrac{1}{r!}\Psi_2^{(r)}(c)\right| \le |2|^{1-3(r-1)} \le |2|^{1-4(r-1)}$ for any $c \equiv 1 \bmod 8$.

Thus, $\left|\dfrac{1}{r!}\Psi^{(r)}(c)\right| \le |2|^{1-4(r-1)}$ for all $r \ge 1$ and

$\left|\dfrac{1}{r!}\Psi^{(r)}(c)\right| \le |2|^{1-3(r-1)}$ for $r \ge 3$.

$\sum_{n=0}^{\infty} \dfrac{\Psi^{(r)}(c)}{r!}(x-c)^r$ converges on $c+16R$.

Apply our result to $m=4$.

Sheet 27 **Concluding remarks (1)**

It is easy to generalize our results to multivariate cases. What is difficult is to show that a given function satisfies our assumptions.

Sheet 28 **Concluding remarks (2)**

	Original SST	Our formulation
Solves	$g(\sigma^{-1}(X), X) = 0$	$X = \sigma^{-1}(f(X))$
Poly. Mul in the inner loop	p+8	p+4

For analysis specific to SST-aided AGM (faster outer loop, $p+8 \to p+5$) and its implementation, we refer to:

P. Gaudry: A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2.
(To appear in ASIACRYPT 2002)