Efficient Point Counting on Curves: Methods and Applications

Garrett Credi

July 18, 2022

Project Goals

High Level: Determine number of points on a curve $\mod p^k$ *quickly*.

Project Goals

High Level: Determine number of points on a curve $\mod p^k$ *quickly*.

Specifically:

- Input: A polynomial $f \in \mathbb{Z}[x, y]$, a prime p, and $k > 0$.
- Output: $N_{p,k}(f) = \left|\left\{\zeta \in \left({}^{\mathbb{Z}}\!/\!_{p^k\mathbb{Z}}\right)^2 \mid f(\zeta) \equiv 0 \mod p^k\right\}\right|$
- Complexity: Polynomial in $deg(f), \log(p)$ and k

Project Goals

High Level: Determine number of points on a curve $\mod p^k$ *quickly*.

Specifically:

- Input: A polynomial $f \in \mathbb{Z}[x, y]$, a prime p, and $k > 0$.
- Output: $N_{p,k}(f) = \left| \left\{ \zeta \in \left(\mathbb{Z}/_{p^k\mathbb{Z}} \right)^2 \mid f(\zeta) \equiv 0 \mod p^k \right\} \right|$
- Complexity: Polynomial in $deg(f), \log(p)$ and k

For the remainder of the talk we denote

$Z_{p,k}(f) = \left\{ \zeta \in \left(\mathbb{Z}/_{p^k\mathbb{Z}} \right)^2 \mid f(\zeta) \equiv 0 \mod p^k \right\}$

Truncation

Important Observation 1: For a given prime p, all the base rings are related.

Truncation

Important Observation 1: For a given prime p, all the base rings are related.

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \xleftarrow{\pi_{p,2}} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\pi_{p,3}} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\pi_{p,4}} \mathbb{Z}/p^4\mathbb{Z} \xleftarrow{\pi_{p,5}} \ldots \longleftarrow \mathbb{Z}_p$$

Where the horizontal maps are 'truncations':

$$\pi_{p,k} : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^{k-1}\mathbb{Z}$$

$$[n] \mapsto [n \mod p^{k-1}]$$

And $\mathbb{Z}_p$ is the 'p-adic integers'.

Beginning Lifting

Consequently, we get maps $\pi_{p,k}(f) : Z_{p,k}(f) \to Z_{p,k-1}(f)$.

Beginning Lifting

Consequently, we get maps $\pi_{p,k}(f) : Z_{p,k}(f) \to Z_{p,k-1}(f)$.
Inductively, $|Z_{p,k}(f)| = \sum_{\zeta \in Z_{p,k-1}(f)} |\pi_{p,k}(f)^{-1}(\zeta)|$.
How can we get information about $|\pi_{p,k}(f)^{-1}(\zeta)|$?

Beginning Lifting

Consequently, we get maps $\pi_{p,k}(f) : Z_{p,k}(f) \to Z_{p,k-1}(f)$.
Inductively, $|Z_{p,k}(f)| = \sum_{\zeta \in Z_{p,k-1}(f)} |\pi_{p,k}(f)^{-1}(\zeta)|$.
How can we get information about $|\pi_{p,k}(f)^{-1}(\zeta)|$? Hensel's Lemma!

Beginning Lifting

Consequently, we get maps $\pi_{p,k}(f) : Z_{p,k}(f) \to Z_{p,k-1}(f)$.
Inductively, $|Z_{p,k}(f)| = \sum_{\zeta \in Z_{p,k-1}(f)} |\pi_{p,k}(f)^{-1}(\zeta)|$.
How can we get information about $|\pi_{p,k}(f)^{-1}(\zeta)|$? Hensel's Lemma!
Firstly, note that $\pi_{p,k}^{-1}(\zeta) = \{\zeta + p^{k-1}d \mid d \in \mathbb{F}_p\}$.

Beginning Lifting

Consequently, we get maps $\pi_{p,k}(f) : Z_{p,k}(f) \to Z_{p,k-1}(f)$.
Inductively, $|Z_{p,k}(f)| = \sum_{\zeta \in Z_{p,k-1}(f)} |\pi_{p,k}(f)^{-1}(\zeta)|$.
How can we get information about $|\pi_{p,k}(f)^{-1}(\zeta)|$? Hensel's Lemma!
Firstly, note that $\pi_{p,k}^{-1}(\zeta) = \{\zeta + p^{k-1}d \mid d \in \mathbb{F}_p\}$. E.g. for $[3] \in {}^{\mathbb{Z}}\!/\!{}_{5^1\mathbb{Z}}$, $\pi_{5,2}^{-1}([3]) =$
$\{[3+0\cdot 5], [3+1\cdot 5], [3+2\cdot 5], [3+3\cdot 5], [3+4\cdot 5]\}$

Hensel Lifting

If we have $\zeta' \in \pi_{p,k}(f)^{-1}(\zeta)$ then $\zeta' = \zeta + p^{k-1} \cdot d$ for $d \in \mathbb{F}_p^2$ (since ζ is a coordinate-pair).

Hensel Lifting

If we have $\zeta' \in \pi_{p,k}(f)^{-1}(\zeta)$ then $\zeta' = \zeta + p^{k-1} \cdot d$ for $d \in \mathbb{F}_p^2$ (since ζ is a coordinate-pair).
So then, when does $f(\zeta + p^{k-1} \cdot d) \equiv 0 \mod p^k$?

Hensel Lifting

If we have $\zeta' \in \pi_{p,k}(f)^{-1}(\zeta)$ then $\zeta' = \zeta + p^{k-1} \cdot d$ for $d \in \mathbb{F}_p^2$ (since ζ is a coordinate-pair).
So then, when does $f(\zeta + p^{k-1} \cdot d) \equiv 0 \mod p^k$?
By Taylor-expanding f about ζ we see that
$f(\zeta + p^{k-1} \cdot d) = f(\zeta) + p^{k-1}(\nabla f)(\zeta) \cdot d + \mathcal{O}(p^k)$.

Hensel Lifting

If we have $\zeta' \in \pi_{p,k}(f)^{-1}(\zeta)$ then $\zeta' = \zeta + p^{k-1} \cdot d$ for $d \in \mathbb{F}_p^2$ (since ζ is a coordinate-pair).
So then, when does $f(\zeta + p^{k-1} \cdot d) \equiv 0 \mod p^k$?
By Taylor-expanding f about ζ we see that
$f(\zeta + p^{k-1} \cdot d) = f(\zeta) + p^{k-1}(\nabla f)(\zeta) \cdot d + \mathcal{O}(p^k)$.
Therefore

$$\zeta + p^{k-1} d \in \pi_{p,k}(f)^{-1}(\zeta) \iff p^{k-1}(\nabla f)(\zeta) \cdot d \equiv -f(\zeta) \mod p^k$$

Recasting Hensel Lifting

Note that, since $\zeta \in Z_{p,k-1}(f)$, $f(\zeta) = p^{k-1} \cdot z$ for some $z \in \mathbb{Z}$.

Recasting Hensel Lifting

Note that, since $\zeta \in Z_{p,k-1}(f)$, $f(\zeta) = p^{k-1} \cdot z$ for some $z \in \mathbb{Z}$. Therefore $f(\zeta + p^{k-1}d) \equiv p^{k-1}(z + (\nabla f)(\zeta) \cdot d) \mod p^k$. So lifting ζ now involves solving the auxiliary equation

$$p^{k-1}(z + (\nabla f)(\zeta) \cdot d) \equiv 0 \mod p^k$$

Recasting Hensel Lifting

Note that, since $\zeta \in Z_{p,k-1}(f)$, $f(\zeta) = p^{k-1} \cdot z$ for some $z \in \mathbb{Z}$. Therefore $f(\zeta + p^{k-1}d) \equiv p^{k-1}(z + (\nabla f)(\zeta) \cdot d) \mod p^k$. So lifting ζ now involves solving the auxiliary equation

$$p^{k-1}(z + (\nabla f)(\zeta) \cdot d) \equiv 0 \mod p^k$$

$$z + (\nabla f)(\zeta) \cdot d \equiv 0 \mod p$$

Recasting Hensel Lifting cont.

$$z + (\nabla f)(\zeta) \cdot d \equiv 0 \mod p$$

Recasting Hensel Lifting cont.

$$z + (\nabla f)(\zeta) \cdot d \equiv 0 \mod p$$

Equation is guaranteed to have p solutions if $(\nabla f)(\zeta) \not\equiv \vec{0} \mod p$.

Recasting Hensel Lifting cont.

$$z + (\nabla f)(\zeta) \cdot d \equiv 0 \mod p$$

Equation is guaranteed to have p solutions if $(\nabla f)(\zeta) \not\equiv \vec{0} \mod p$.
I.e. $\zeta \mod p$ is a *non-singular* point on $f \mod p$!

Recasting Hensel Lifting cont.

$$z + (\nabla f)(\zeta) \cdot d \equiv 0 \mod p$$

Equation is guaranteed to have p solutions if $(\nabla f)(\zeta) \not\equiv \vec{0} \mod p$.
I.e. $\zeta \mod p$ is a *non-singular* point on $f \mod p$!
Instead of needing all the $\mod p^k$ information, the behavior of a $\mathbb{F}_p$ root $\bar{\zeta}$ is enough to determine how higher powers lift.

Recasting Hensel Lifting cont.

$$z + (\nabla f)(\zeta) \cdot d \equiv 0 \mod p$$

Equation is guaranteed to have p solutions if $(\nabla f)(\zeta) \not\equiv \vec{0} \mod p$.
I.e. $\zeta \mod p$ is a *non-singular* point on $f \mod p$!
Instead of needing all the $\mod p^k$ information, the behavior of a $\mathbb{F}_p$ root $\bar{\zeta}$ is enough to determine how higher powers lift.
What if we have a singular $\mathbb{F}_p$ root?

The Case of Singular Roots

Given an $\mathbb{F}_p$ root $\zeta = (x, y)$, we know that its lifts to ${}^{\mathbb{Z}}\!/_{p^k\mathbb{Z}}$ must be of the form $\zeta + pd, \ d = (x_0, y_0) \in \left({}^{\mathbb{Z}}\!/_{p^{k-1}\mathbb{Z}}\right)^2$.

The Case of Singular Roots

Given an $\mathbb{F}_p$ root $\zeta = (x, y)$, we know that its lifts to $\mathbb{Z}/_{p^k\mathbb{Z}}$ must be of the form $\zeta + pd,\ d = (x_0, y_0) \in \left(\mathbb{Z}/_{p^{k-1}\mathbb{Z}}\right)^2$.

$$f(\zeta + pd) = f(\zeta) + \sum_{n=1}^{\infty} p^n \sum_{i+j=n} \frac{1}{i!j!} \frac{\partial^n f}{\partial x^i \partial y^j}(\zeta) x_0^i y_0^j$$

Similarly to how we factored out a p^{k-1} in the previous slide to reduce f, we define $s(f, \zeta) = \min_{i,j\geq 0}\{i + j + \frac{1}{i!j!} \frac{\partial^n f}{\partial x^i \partial y^j}(\zeta)\}$

The Case of Singular Roots

Given an $\mathbb{F}_p$ root $\zeta = (x, y)$, we know that its lifts to ${}^{\mathbb{Z}}\!/\!_{p^k\mathbb{Z}}$ must be of the form $\zeta + pd,\ d = (x_0, y_0) \in \left({}^{\mathbb{Z}}\!/\!_{p^{k-1}\mathbb{Z}}\right)^2$.

$$f(\zeta + pd) = f(\zeta) + \sum_{n=1}^{\infty} p^n \sum_{i+j=n} \frac{1}{i!j!} \frac{\partial^n f}{\partial x^i \partial y^j}(\zeta) x_0^i y_0^j$$

Similarly to how we factored out a p^{k-1} in the previous slide to reduce f, we define $s(f, \zeta) = \min_{i,j \geq 0}\{i + j + \frac{1}{i!j!} \frac{\partial^n f}{\partial x^i \partial y^j}(\zeta)\}$

This is so that $p^{s(f,\zeta)} \parallel f(\zeta + pd)$ (i.e. perfectly divides).

Point Counting Formula

With that notation, let $f_{k,\zeta}$ be such that $f(\zeta + pd) \equiv p^{s(f,\zeta)} f_{k,\zeta}(d) \mod p^k$.

Point Counting Formula

With that notation, let $f_{k,\zeta}$ be such that $f(\zeta + pd) \equiv p^{s(f,\zeta)} f_{k,\zeta}(d) \mod p^k$.
If $s(f,\zeta) \geq k$ then we have $p^{2(k-1)}$ many lifts as every point $\zeta' \in \left(\mathbb{Z}/_{p^k\mathbb{Z}}\right)^2$ of the form $\zeta + pd, d \in \left(\mathbb{Z}/_{p^{k-1}\mathbb{Z}}\right)$ satisfies the congruence.

Point Counting Formula

With that notation, let $f_{k,\zeta}$ be such that $f(\zeta + pd) \equiv p^{s(f,\zeta)} f_{k,\zeta}(d) \mod p^k$.
If $s(f,\zeta) \geq k$ then we have $p^{2(k-1)}$ many lifts as every point $\zeta' \in \left(\mathbb{Z}/_{p^k\mathbb{Z}}\right)^2$ of the form $\zeta + pd, d \in \left(\mathbb{Z}/_{p^{k-1}\mathbb{Z}}\right)$ satisfies the congruence.
Similarly if $s(f,\zeta) < k$ for every root in $Z_{p,k-s(f,\zeta)}(f_{k,\zeta})$ there are $p^{2(s(f,\zeta)-1)}$ lifts by considering p-adic digits.

Point Counting Formula

With that notation, let $f_{k,\zeta}$ be such that $f(\zeta + pd) \equiv p^{s(f,\zeta)} f_{k,\zeta}(d) \mod p^k$.
If $s(f,\zeta) \geq k$ then we have $p^{2(k-1)}$ many lifts as every point $\zeta' \in \left({}^{\mathbb{Z}}\!/\!_{p^k\mathbb{Z}}\right)^2$ of the form $\zeta + pd, d \in \left({}^{\mathbb{Z}}\!/\!_{p^{k-1}\mathbb{Z}}\right)$ satisfies the congruence.
Similarly if $s(f,\zeta) < k$ for every root in $Z_{p,k-s(f,\zeta)}(f_{k,\zeta})$ there are $p^{2(s(f,\zeta)-1)}$ lifts by considering p-adic digits. Thus, letting $n_s(f) = |\{\zeta \in Z_{p,1}(f) | (\nabla f)(\zeta) \neq \vec{0}\}|$ we have:

Point Counting Recurrence Formula

$$|Z_{p,k}(f)| = n_s(f)p^{k-1} + \sum_{\substack{\zeta \in Z_{p,1}(f) \\ s(f,\zeta) \geq k}} p^{2(k-1)} + \sum_{\substack{\zeta \in Z_{p,1}(f) \\ 2 \leq s(f,\zeta) < k}} p^{2(s(f,\zeta)-1)} |N_{p,k-s(f,\zeta)}(f_{k,\zeta})|$$

Examining $Z_{p,1}(f)$

The recurrence involves knowing how many non-singular points there are on $f \mod p$ as well as knowing the singular roots.
To determine the number of total points on $Z_{p,1}(f)$ we can use an algorithm thanks to (Harvey):

Examining $Z_{p,1}(f)$

The recurrence involves knowing how many non-singular points there are on $f \mod p$ as well as knowing the singular roots.
To determine the number of total points on $Z_{p,1}(f)$ we can use an algorithm thanks to (Harvey):

THEOREM 3.1 (Trace formula). *Let $\bar{F} \in \mathbf{F}_q[x]_d$ and let X be the hypersurface in $\mathbf{T}^n_{\mathbf{F}_q}$ cut out by $\bar{F}$. Let r, λ and τ be positive integers satisfying*

$$\tau \geq \frac{\lambda}{(p-1)ar}. \tag{3.3}$$

Let $F \in \mathbf{Z}_q[x]_d$ be any lift of $\bar{F}$. Then

$$|X(\mathbf{F}_{q^r})| = (q^r - 1)^n \sum_{s=0}^{\lambda+\tau-1} \alpha_s \operatorname{tr}(A^{ar}_{F^s}) \pmod{p^\lambda},$$

where

$$\alpha_s = (-1)^s \sum_{t=0}^{\tau-1} \binom{-\lambda}{t} \binom{\lambda}{s-t} \in \mathbf{Z},$$

and where A_{F^s} is regarded as a linear operator on $\mathbf{Z}_q[x]_{ds}$.

Figure: (Harvey)p. 9

Simplifying Harvey?

Unfortunately, the algorithm Harvey describes runs in $\sqrt{p}\log(p)^{1+\epsilon}$-time (ignoring the degree of f).

Simplifying Harvey?

Unfortunately, the algorithm Harvey describes runs in $\sqrt{p}\log(p)^{1+\epsilon}$-time (ignoring the degree of f).
Yet many of the terms involved in the theorem can be simplified in the case of point counting over $\mathbb{F}_p$. Perhaps it can speed up the algorithm?

Simplifying Harvey?

Unfortunately, the algorithm Harvey describes runs in $\sqrt{p}\log(p)^{1+\epsilon}$-time (ignoring the degree of f).
Yet many of the terms involved in the theorem can be simplified in the case of point counting over $\mathbb{F}_p$. Perhaps it can speed up the algorithm?
The central term in the theorem is $tr(A^{ar}_{F^s})$, where F is the homogenization of f (i.e. $F \in \mathbb{Z}[X,Y,Z], F(X,Y,Z) = Z^{deg(f)}f(\frac{X}{Z},\frac{Y}{Z})$).

Simplifying Harvey? cont.

Crucially, Harvey provides a lemma that provides a matrix representation for $A^{ar}_{F^s}$.

Simplifying Harvey? cont.

Crucially, Harvey provides a lemma that provides a matrix representation for $A^{ar}_{F^s}$.
Say $deg(F^s) = d$. The matrix M is indexed by degree d monomials, so for $u, v \in \mathbb{Z}[X, Y, Z]_d$ (after identifying a monomial with their exponent vector), $M_{(u,v)} = (F^{s(p-1)})_{(pv-u)}$.

Simplifying Harvey? cont.

Crucially, Harvey provides a lemma that provides a matrix representation for $A^{ar}_{F^s}$.
Say $deg(F^s) = d$. The matrix M is indexed by degree d monomials, so for $u, v \in \mathbb{Z}[X, Y, Z]_d$ (after identifying a monomial with their exponent vector), $M_{(u,v)} = (F^{s(p-1)})_{(pv-u)}$.

$$tr(A^{ar}_{F^s}) = tr(M) = \sum_{u \in \mathbb{Z}[X,Y,Z]_d} (F^{s(p-1)})_{(p-1)u}$$

Example Trace Computation

For example, if $F = ZY^2 - X^3 - ZX^2, s = 1, p = 3$ then $F^{s(p-1)} = X^6 + 2X^5Z - 2X^3Y^2Z + X^4Z^2 - 2X^2Y^2Z^2 + Y^4Z^2 = (X^6 + X^4Z^2 - 2X^2Y^2Z^2 + Y^4Z^2) + 2X^5Z - 2X^3Y^2Z$.

Example Trace Computation

For example, if $F = ZY^2 - X^3 - ZX^2, s = 1, p = 3$ then
$F^{s(p-1)} = X^6 + 2X^5Z - 2X^3Y^2Z + X^4Z^2 - 2X^2Y^2Z^2 + Y^4Z^2 =$
$(X^6 + X^4Z^2 - 2X^2Y^2Z^2 + Y^4Z^2) + 2X^5Z - 2X^3Y^2Z.$
Trace is $1 + 1 - 2 + 1 = 1.$

Harvey Problems

However, I was not able to derive a $\log(p)$ time algorithm to determine this specific coefficient sum.

Harvey Problems

However, I was not able to derive a $\log(p)$ time algorithm to determine this specific coefficient sum.
Major Problem: Like in the previous example the monomials present in F^s were $\{ZY^2, X^3, ZX^2\}$ but the monomial whose $(p-1)$ powers appeared in $F^{s(p-1)}$ were $\{ZY^2, X^3, ZX^2, XYZ\}$.
Determining when monomials 'interacted' to give rise to new monomials in the exponentiation was very difficult.

Harvey Problems

However, I was not able to derive a $\log(p)$ time algorithm to determine this specific coefficient sum.
Major Problem: Like in the previous example the monomials present in F^s were $\{ZY^2, X^3, ZX^2\}$ but the monomial whose $(p-1)$ powers appeared in $F^{s(p-1)}$ were $\{ZY^2, X^3, ZX^2, XYZ\}$.
Determining when monomials 'interacted' to give rise to new monomials in the exponentiation was very difficult.
Thus, in a similar vein to previous REU's, using the $\sqrt{p}$ algorithm will have to suffice.

Too Many Singular Points

To recall, we had to iterate over the $\mathbb{F}_p$ singular points of f in the point counting formula. Now, for nice curves, the number of singular points is generally sublinear in p (i.e. the ideal $\langle f, \partial_x f, \partial_y f \rangle$ is a zero dimensional ideal).

Too Many Singular Points

To recall, we had to iterate over the $\mathbb{F}_p$ singular points of f in the point counting formula. Now, for nice curves, the number of singular points is generally sublinear in p (i.e. the ideal $\langle f, \partial_x f, \partial_y f \rangle$ is a zero dimensional ideal).
Unfortunately, in cases where $f \mod p$ is not a square-free polynomial, the number of singular points is $\mathcal{O}(p)$.

(g, p, k) Valuative Decompositions

Say we have a $g \in \mathbb{F}_p[x, y]$ such that $g^2 | f \mod p$. Decompose f in the following manner: $f = \sum_{i=0}^{k-1} p^i g^{e_i} h_i$.

(g, p, k) Valuative Decompositions

Say we have a $g \in \mathbb{F}_p[x, y]$ such that $g^2 | f \mod p$. Decompose f in the following manner: $f = \sum_{i=0}^{k-1} p^i g^{e_i} h_i$.
One of the sub-goals of this project was, in such a case as above, to determine $|Z_{p,k}(f) \cap Z_{p,k}(g)|$.

(g, p, k) Valuative Decompositions

Say we have a $g \in \mathbb{F}_p[x, y]$ such that $g^2 | f \mod p$. Decompose f in the following manner: $f = \sum_{i=0}^{k-1} p^i g^{e_i} h_i$.
One of the sub-goals of this project was, in such a case as above, to determine $|Z_{p,k}(f) \cap Z_{p,k}(g)|$.
If $\forall i, e_i \geq 1$, then $|Z_{p,k}(f) \cap Z_{p,k}(g)| = |Z_{p,k}(g)|$.

(g,p,k) Valuative Decompositions

Say we have a $g \in \mathbb{F}_p[x,y]$ such that $g^2 | f \mod p$. Decompose f in the following manner: $f = \sum_{i=0}^{k-1} p^i g^{e_i} h_i$.
One of the sub-goals of this project was, in such a case as above, to determine $|Z_{p,k}(f) \cap Z_{p,k}(g)|$.
If $\forall i, e_i \geq 1$, then $|Z_{p,k}(f) \cap Z_{p,k}(g)| = |Z_{p,k}(g)|$.
Otherwise, $f = \sum_{\substack{0 \leq i < p \\ e_i \neq 0}} p^i g^{e_i} h_i + \sum_{\substack{0 \leq i < p \\ e_i = 0}} p^i h_i$.
To count how many $\zeta \in Z_{p,k}(f) \cap Z_{p,k}(g)$, notice if $g(\zeta) \equiv 0 \mod p^k$ then $f(\zeta) \equiv \sum_{\substack{0 \leq i < p \\ e_i = 0}} p^i h_i(\zeta)$.
Set $\nu = \min\{i | e_i = 0\}$.

Current Approach to Intersection Counting

Therefore, the number of solutions to the system

$$\begin{cases} f \equiv 0 \mod p^k \\ g \equiv 0 \mod p^k \end{cases}$$

is the same as the number of solutions to the system

$$\begin{cases} p^{-\nu} \sum\limits_{\substack{0 \le i < p \\ e_i = 0}} p^i h_i \equiv 0 \mod p^{k-\nu} \\ g \equiv 0 \mod p^k \end{cases}$$

References

Harvey, David, Computing zeta functions of arithmetic schemes, 2014. doi:10.48550/ARXIV.1402.3439.