Extending the special number field sieve

Oliver Schirokauer

September 20, 2006

Definition The *weight* of an integer N is the smallest w such that

$$N = \sum_{i=1}^{w} \epsilon_i 2^{c_i},$$

with $\epsilon_i \in \{1, -1\}$.

It is tempting to use such primes in cryptographic protocols, for example in pairing based cryptography. (Solinas)

Question When the security of a system depends on the difficulty of computing discrete logarithms in a finite field of characteristic p, how is that security affected by the weight of p?

Example. (Koblitz, Menezes) Let

$$p = 2^{15474} - 2^{14954} + 2^{14432} + 1$$

and assume we are interested in computing discrete logarithms in $\mathbb{F}_p$.

The "NFS-security" in this case is 13180 bits. In other words, you might as well be working with a general prime of 13180 bits.

The number field sieve for computing logarithms in a finite field F:

i) Find two number rings $\mathcal{O}_1$ and $\mathcal{O}_2$ and ring homomorphisms

$$\phi_1 : \mathcal{O}_1 \to F$$

$$\phi_2 : \mathcal{O}_2 \to F.$$

ii) Search for many pairs $(\delta_1, \delta_2) \in \mathcal{O}_1 \times \mathcal{O}_2$ such that

* $\phi_1(\delta_1) = \phi_2(\delta_2)$
* the norms of δ_1 and δ_2 in $\mathbb{Z}$ are smooth.

iii) Use linear algebra to find discrete logarithms.

The running time of the method depends on the size of the norms being tested for smoothness.

Assume $|F| = p$.

Let $d + 1$ be the sum of the degrees over $\mathbb{Q}$ of the fraction fields of $\mathcal{O}_1$ and $\mathcal{O}_2$. Let M^2 be the number of smoothness candidates tested. In the SNFS (for primes of the from $r^e + s$ with r and s small), the numbers tested for smoothness are bounded by

$$M^{d+1} p^{\frac{1}{d}}.$$

The resulting conjectural running time, for $p \to \infty$, is

$$L_p[1/3; (32/9)^{1/3} + o(1)].$$

($L_p[s; c] = \exp(c(\log\, p)^s (\log \log\, p)^{1-s}$.)

In the general case, the numbers tested for smoothness are bounded by

$$M^{d+1} p^{\frac{2}{d+2}}.$$

The resulting conjectural running time is

$$L_p[1/3; (64/9)^{1/3} + o(1)],$$

for $p \to \infty$.

In the low-weight example given earlier, we can let

$$\mathcal{O}_1 = \mathbb{Z}$$

and

$$\mathcal{O}_2 = \mathbb{Z}[\alpha],$$

where α is a root of

$$f = (2^{520} - 1)x^{14} + 2^{547}x^{13} + 1.$$

Note that $p | f(2^{1069})$.

Let ϕ_1 be the usual projection, and let ϕ_2 be the map that sends α to $2^{1069} \bmod p$.

The pairs tested for smoothness are

$$a - b2^{1069}, a - b\alpha,$$

with $a, b \in \mathbb{Z}$. The norm of $a - b\alpha$ is

$$b^{14} f(a/b).$$

We find that the numbers tested for smoothness are bounded by

$$M^{15}2^{1619}.$$

This value is between the SNFS and general NFS bounds given earlier.

More specific questions:

What is the running time of our method as a function of the weight?

Is the weight a good predictor of the running time for a particular prime?

Assume

$$p = \sum_{i=1}^{w} \epsilon_i 2^{c_i}.$$

For a given e, we can find a polynomial f such that

* $f(2^e) \equiv 0 \bmod p$
* the coefficients of f are bounded by $e - \gamma$, where γ is the largest gap occurring in the sequence obtained by listing in increasing order the residues of the c_i mod e. (We include 0 and e in the sequence.)

Back to our example:

$$p = 2^{15474} - 2^{14954} + 2^{14432} + 1$$

$$e = 1069.$$

The sequence of residues is

$$1, 508, 535, 1057, 1069.$$

$$(1, \overline{15474}, \overline{14432}, \overline{14954}, 1069)$$

The largest gap is between 535 and 1057.

We find that $2^{12}p =$

$2^{520}(2^{1069})^{14} - (2^{1069})^{14} + 2^{547}(2^{1069})^{13} + 1.$

Rough analysis:

In the worst case, the largest gap is

$$\frac{e}{w-1.}$$

Let

$$\theta = \frac{2w-3}{w-1}.$$

In the worst case, the numbers tested for smoothness are bounded by

$$M^{d+1}2^{2e-\frac{e}{w-1}} \approx M^{d+1}p^{\frac{\theta}{d}}.$$

The resulting conjectural running time is

$$L_p[1/3; (32\theta/9)^{1/3} + o(1)],$$

for $p \to \infty$.

A closer look reveals that one can always do better than a gap size of $e/(w-1)$. However, one cannot improve much on the running time just given.

Let

$$\tau = \frac{\sqrt{2}w - w\sqrt{2} + 1}{w - 1}.$$

There exists an infinite set of integers of weight w with the property that the conjectural running time of our method is at least

$$L_p[1/3; (32\tau^2/9)^{1/3} + o(1)],$$

for $p \to \infty$.

	$(32\tau^2/9)^{1/3}$	$(32\theta/9)^{1/3}$
$w = 2$	1.526	1.526
$w = 3$	1.730	1.747
$w = 4$	1.796	1.810
$w = 5$	1.828	1.839
$w = 6$	1.847	1.857
$w = 7$	1.860	1.868
$w = 8$	1.869	1.876
$w = 9$	1.876	1.882
$w = 10$	1.881	1.887

These results are deceptive.

For a given weight w, the asymptotic gain over the general NFS is only realized for large p.

The gap in the sequence of residues is usually much larger than $e/(w-1)$.

Proposition. Let S be the set of sequences of length $w-2$ of non-negative integers less than e. For $s \in S$, let $\gamma(s)$ be the largest gap in the sequence obtained by ordering the elements of s, together with 0 and e. Then the average value of $\gamma(s)$ is

MESS.

The chart below gives values of

$$\frac{\text{MESS}}{e}$$

and the value $1/(w-1)$ for comparison.

	$e = 200$	$e = 1000$	$e = \infty$	$\frac{1}{w-1}$
$w = 3$	.753	.751	.750	.500
$w = 4$	.604	.610	.611	.333
$w = 5$	.508	.518	.521	.250
$w = 6$	.439	.453	.457	.200
$w = 7$	.386	.404	.408	.167
$w = 8$	.340	.364	.370	.143
$w = 9$	.301	.332	.340	.125
$w = 10$	.268	.305	.314	.111

End of Part I.

Part II: A modification for logarithms in non-prime fields:

Example (degree 2). Let

$$p = 2^{520} + 2^{230} + c,$$

where $c = 2^{60} + 2^{20} + 2^9 + 13$.

Observe that 2 is a quadratic non-residue mod p.

Assume we want to compute logarithms in $\mathbb{F}_{p^2}$.

Option 1: Using the method already discussed, obtain

$$f = 2^{60}x^5 + 2^{46}x^2 + c.$$

Let

$$\mathcal{O}_1 = \mathbb{Z}[\sqrt{2}]$$

$$\mathcal{O}_2 = \mathbb{Z}[\sqrt{2}, \alpha],$$

where $f(\alpha) = 0$.

Test pairs of the form

$$(a_1 + a_2\sqrt{2}) - (b_1 + b_2\sqrt{2})2^{92},$$
$$(a_1 + a_2\sqrt{2}) - (b_1 + b_2\sqrt{2})\alpha,$$

with a_1, b_1, a_2, b_2 bounded by $\sqrt{M}$ in absolute value.

The norm bound is

$$M^6 2^{304}.$$

Option 2: Joux, Lercier, Smart, and Vercauteren observe that we can let $\mathcal{O}_1$ be the ring obtained by adjoining to $\mathbb{Z}$ a root of an irreducible quadratic $f \in \mathbb{Z}[x]$ and then let $\mathcal{O}_2$ be obtained by adjoining to $\mathbb{Z}$ a root of an irreducible polynomial g of degree ≥ 2, having the property that f divides g mod p.

Modification: Write

$$p = \sqrt{2}^{1040} + \sqrt{2}^{460} + c.$$

Applying the same procedure as before, we obtain

$$g = 2^{59}x^4 + x^2 + 2c,$$

which has $\sqrt{2}^{231}$ as a root mod p.

In other words, g is divisible by $x^2 - 2^{231}$ mod p.

Let β be a root of g.

Assuming that we test for smoothness pairs of the form

$$a - b\sqrt{2}^{231}, a - b\beta,$$

with $a, b \in \mathbb{Z}$ bounded by M in absolute value, we obtain a norm bound of

$$M^6 2^{292}.$$

We have an improvement ... and we did not even take into account, in the first option, the contribution coming from the basis of $\mathbb{Z}[\sqrt{2}]$ and the cost of working in a degree 10 extension.

Example (SNFS).

Let

$$p = \frac{3^{60} + 5}{2}$$

and consider the logarithm problem in $\mathbb{F}_{p^{18}}$.

Note that $x^{18} - 3$ is irreducible mod p.

Option 1: Let $f = x^5 + 5$, in which case $f(3^{12}) \equiv 0 \bmod p$.

Let $\mathcal{O}_1$ be any ring with residue field $\mathbb{F}_{p^{18}}$. Let $\mathcal{O}_2 = \mathcal{O}_1[\alpha]$, where α is a root of f.

We test for smoothness pairs of the form

$$a - b3^{12}, a - b\alpha,$$

with $a, b \in \mathcal{O}_1$.

If we choose the M^2 smallest a, b, we obtain a norm bound of

$$M^6 (p^{18})^{1/5}.$$

Option 2: Let $\mu = \sqrt[18]{3}$, and write

$$2p = \mu^{1080} + 5.$$

Let

$$f = x^4 + 5\mu^4 = x^4 + 5(\sqrt[9]{3})^2,$$

and observe that μ^{271} is a root of f mod p.

We let $\mathcal{O}_1 = \mathbb{Z}[\mu]$ and $\mathcal{O}_2 = \mathbb{Z}[\sqrt[9]{3}, \alpha]$, where α is a root of f.

We test for smoothness pairs of the form

$$a - b\mu^{271}, a - b\alpha,$$

with a, b in $\mathbb{Z}[\sqrt[9]{3}]$.

If we choose the M^2 smallest such a, b, we obtain a norm bound of

$$M^6(p^{18})^{1/4}.$$

The first bound is clearly much better than the second. However, in the former case, the extensions being used are of degree 18 and 90. In the latter case they are of degree 18 and 36.

The increase in norm size resulting from working in the degree 90 field may outweigh the difference between these bounds.

Example. (Barreto, Naehrig) Let

$$c = 2^{80} + 99$$

$$f = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$

$$p = f(c).$$

Assume we are interested in computing logarithms in $\mathbb{F}_{p^{12}}$.

Note that c is a quadratic non-residue mod p.

Let $\mathcal{O}_1$ be any number ring with residue field $\mathbb{F}_{p^{12}}$. It is tempting to run the NFS with $\mathcal{O}_2 = \mathcal{O}_1[\alpha]$, where α is a root of f. The pairs tested for smoothness would then be

$$a - bc, a - b\alpha,$$

with $a, b \in \mathcal{O}_1$.

The norm bound for M^2 candidates would be

$$M^5 c^{12} \approx M^5 (p^{12})^{1/4}.$$

This is the SNFS bound for $d = 4$, with p replaced by p^{12}.

However, for the p under consideration, the optimal value of d is 8.

Let $\mathcal{O}_1$ be a number ring containing $\sqrt{c}$ and having $\mathbb{F}_{p^{12}}$ as a residue field.

Let $g = 36x^8 + 36x^6 + 24x^4 + 6x^2 + 1$ and let $\mathcal{O}_2 = \mathcal{O}_1[\beta]$, where β is a root of g.

We test for smoothness pairs

$$a - b\sqrt{c}, a - b\beta,$$

where $a, b \in \mathcal{O}_1$.

The norm bound for M^2 candidates is

$$M^9 c^6 \approx M^9 (p^{12})^{1/8}.$$

Thus we have again taken advantage of the special representation of p.

Of course, this bound completely ignores the significant impact of working in extensions of degree 12 and 96.

We obtain the analogous result, under the assumption that c is an appropriate non-residue mod p, for various values of d.

Below is a list of all cases. For each degree, the accompanying range indicates the field sizes, in bits, for which that value of d is optimal. Note that these values are obtained from an asymptotic formula and are very rough. In particular, for $d = 4$, I expect they are too low.

$d = 4$	$250 - 500$
$d = 8$	$3200 - 4700$
$d = 12$	$13,500 - 17,500$
$d = 16$	$36,500 - 44,500$
$d = 24$	$144,000 - 164,000$
$d = 48$	$1,430,000 - 1,520,000$