SNFS Poly

Sean A. Irvine

December 16, 2018

The number field sieve (NFS) requires two distinct irreducible polynomials, f and g, and an integer m such that $f(m) = g(m) = 0 (\mathrm{mod}\, N)$ where N is the number to be factored. For sieving to be efficient the coefficients of f and g should be small and they should both have low degree. For certain numbers it is possible to use algebraic methods to select the polynomials.

In what follows, methods for selecting polynomials suitable for factorization of Fibonacci and Lucas numbers are presented.

Theorem 1 *Let $\alpha = \frac{1}{2}(1+\sqrt{5})$ and $\beta = \frac{1}{2}(1-\sqrt{5})$ be the roots of x^2-x-1. Then the nth Fibonacci number can be expressed*

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

If n is even, then F_n easily splits as $F_{2m} = F_m L_m$ where L_m is the mth Lucas number. Thus, in factoring Fibonacci numbers only odd n need be considered.

It is possible to generate the required sieving polynomials from Theorem **??**. We commence with a construction which works for any odd n not divisible by 5 but for which the resulting polynomial is not always the best choice. Later, we will exhibit better polynomials for the case where n has a small prime divisor.

Let $n \geq 3$ and $n = 5k + r$ where $r \in \{\pm 1, \pm 2\}$. By Theorem **??**

$$\begin{aligned} \alpha^k - \beta^k &= F_k(\alpha - \beta), \\ \alpha^r \alpha^k - \beta^r \beta^k &= F_{k+r}(\alpha - \beta). \end{aligned}$$

Solving for α^k and β^k gives

$$\begin{aligned} \alpha^k &= \frac{\alpha - \beta}{\alpha^r - \beta^r}(F_{k+r} - \beta^r F_k) \\ \beta^k &= \frac{\alpha - \beta}{\alpha^r - \beta^r}(F_{k+r} - \alpha^r F_k) \end{aligned}$$

Let $X = F_{k+r}$ and $Y = F_k$. Then, since $\alpha^n = \alpha^r(\alpha^k)^5$,

$$\alpha^n = \frac{\alpha^r(\alpha-\beta)^5}{(\alpha^r-\beta^r)^5}(X^5 - 5\beta^r Y X^4 + 10\beta^{2r} Y^2 X^3 - 10\beta^{3r} Y^3 X^2 + 5\beta^{4r} Y^4 X - \beta^{5r} Y^5)$$

Similarly,

$$\beta^n = \frac{\beta^r(\alpha-\beta)^5}{(\alpha^r-\beta^r)^5}(X^5 - 5\alpha^r Y X^4 + 10\alpha^{2r} Y^2 X^3 - 10\alpha^{3r} Y^3 X^2 + 5\alpha^{4r} Y^4 X - \alpha^{5r} Y^5)$$

Fixing r yields the following sieving polynomials:

- $r = -2$: $f(x) = x^5 - 10x^3 + 30x^2 - 40x + 21$.
- $r = -1$: $f(x) = x^5 + 10x^3 + 10x^2 + 10x + 3$.
- $r = 1$: $f(x) = x^5 + 10x^3 - 10x^2 + 10x - 3$.
- $r = 2$: $f(x) = x^5 - 10x^3 + 30x^2 - 40x + 21$.

In each case the linear polynomial is $g(x) = F_k x - F_{k+r}$ and the common root is $m = F_{k+r}F_k^{-1} \pmod N$ where N is the number to be factored (that is, $N = F_n/M$ where M is a product of known factors of F_n).

When n has a small prime factor it is possible to get better polynomials. Suppose $n = pm$ where $p \in \{3, 5, 7, 11, 13\}$ and consider F_{pm}/F_m:

$$\begin{aligned} M &= F_{pm}/F_m \\ &= \frac{\alpha^{pm} - \beta^{pm}}{\alpha - \beta} \Big/ \frac{\alpha^m - \beta^m}{\alpha - \beta} \\ &= \frac{\alpha^{pm} - \beta^{pm}}{\alpha^m - \beta^m} \\ &= \sum_{i=0}^{p-1} \beta^{mi}\alpha^{(p-i-1)m} \end{aligned}$$

When $p = 3$ this gives $M = \alpha^{2m} + \beta^m\alpha^m + \beta^{2m}$. Writing $m = 3k + r$ where $r \in \{0, 1, 2\}$ gives

$$\begin{aligned} M &= \alpha^{6k+2r} + \alpha^{3k+r}\beta^{3k+r} + \beta^{6k+2r} \\ &= \alpha^{2r}(F_{k+1} - \beta F_k)^6 + \alpha^r\beta^r(F_{k+1} - \beta F_k)^3(F_{k+1} - \alpha F_k)^3 + \beta^{2r}(F_{k+1} - \alpha F_k)^6 \end{aligned}$$

where we have used $\alpha^k = F_{k+1} - \beta F_k$ and $\beta^k = F_{k+1} - \alpha F_k$ from which (after some tedious expansions) the following sieving polynomial emerges

$$\begin{gathered} (\alpha^{2r} + \beta^{2r} + (-1)^r)F_{k+1}^6 \\ -3(2\beta\alpha^{2r} + 2\alpha\beta^{2r} + (-1)^r)F_{k+1}^5F_k \\ +15(\beta^2\alpha^{2r} + \alpha^2\beta^{2r})F_{k+1}^4F_k^2 \\ -5(4\beta^3\alpha^{2r} + 4\alpha^3\beta^{2r} - (-1)^r)F_{k+1}^3F_k^3 \\ +15(\beta^4\alpha^{2r} + 2\alpha^4\beta^{2r} + (-1)^r)F_{k+1}^2F_k^4 \\ -3(2\beta^5\alpha^{2r} + 2\alpha^5\beta^{2r} + (-1)^r)F_{k+1}F_k^5 \\ +(\beta^6\alpha^{2r} + \alpha^6\beta^{2r} - (-1)^r)F_k^6. \end{gathered}$$

Taking the linear polynomial as $g(x) = F_k x - F_{k+1}$, we obtain the following polynomials

- $r = 0$: $f(x) = x^6 - 9x^5 + 45x^4 - 75x^3 + 105x^2 - 63x + 17$.
- $r = 1$: $f(x) = 2x^6 + 9x^5 + 30x^4 - 25x^3 + 45x^2 - 21x + 8$.
- $r = 2$: $f(x) = 8x^6 + 21x^5 + 45x^4 + 25x^3 + 30x^2 + 9x + 2$.

When $p = 5$,

$$M = \alpha^{4m} + \alpha^{3m}\beta^m + \alpha^{2m}\beta^{2m} + \alpha^m\beta^{3m} + \beta^{4m}$$

which noting $\alpha^m = F_{m+1} - \beta F_m$ and $\beta^m = F_{m+1} - \alpha F_m$ yields the homogeneous polynomial

$$5F_{m+1}^4 + 10F_{m+1}^3F_m + 20F_{m+1}^2F_m^2 + 15F_{m+1}F_m^3 + 5F_m^3,$$

yielding the sieving polynomials

$$\begin{aligned} f(x) &= 5x^4 - 10x^3 + 20x^2 - 15x + 5 \\ g(x) &= F_m x - F_{m+1} \end{aligned}$$

When $p = 7$, a similar but more protracted expansion gives a sixth degree polynomial

$$\begin{aligned} f(x) &= 7x^6 - 21x^5 + 70x^4 - 105x^3 + 105x^2 - 56x + 13 \\ g(x) &= F_m x - F_{m+1} \end{aligned}$$

When $p = 11$ or $p = 13$ a slightly different approach is used to express F_{pm}/F_m as a polynomial in F_m^2. This is achieved by using the multiple-angle formula

$$F_{km} = \sum_{i=0}^{\lfloor k/2 \rfloor} (-)^{in} \frac{k}{k-i} \binom{k-i}{i} 5^{\lfloor k/2 \rfloor - i} F_m^{k-2i}$$

hence

$$F_{km}/F_m = \sum_{i=0}^{\lfloor k/2 \rfloor} (-)^{in} \frac{k}{k-i} \binom{k-i}{i} 5^{\lfloor k/2 \rfloor - i} F_m^{k-2i-1}.$$

When $p = 11$ and m odd this is

$$3125F_m^{10} - 6875F_m^8 + 5500F_m^6 - 1925F_m^4 + 275F_m^2 - 11.$$

When $p = 13$ and m odd this is

$$15625F_m^{12} - 40625F_m^{10} + 40625F_m^8 - 19500F_m^6 + 4550F_m^4 - 455F_m^2 + 13.$$

[what should the linear polys be?]

Polynomials for Lucas numbers divisible by small primes are found obtained using the same techniques used for Fibonacci numbers. Suppose $n = pm$ where $p \in \{3, 5, 7, 11, 13\}$, then

$$\begin{aligned} M &= L_{pm}/L_m \\ &= \frac{\alpha^{pm} + \beta^{pm}}{\alpha^m + \beta^m} \\ &= \sum_{i=0}^{p-1} (-1)^i \beta^{mi} \alpha^{(p-i-1)m} \end{aligned}$$

When $p = 3$ this gives $M = \alpha^{2m} - \alpha^m\beta^m + \beta^{2m}$. Writing $m = 3k + r$, where $r \in \{0, 1, 2\}$ gives

$$\begin{aligned} M &= \alpha^{6k+2r} - \alpha^{3k+r}\beta^{3k+r} + \beta^{6k+2r} \\ &= \alpha^{2r}(F_{k+1} - \beta F_k)^6 - \alpha^r\beta^r(F_{k+1} - \beta F_k)^3(F_{k+1} - \alpha F_k)^3 + \beta^{2r}(F_{k+1} - \alpha F_k)^6 \end{aligned}$$

Fixing r gives the following polynomials

- $r = 0$: $f(x) = x^6 - 3x^5 + 45x^4 - 85x^3 + 105x^2 - 63x + 19$,
- $r = 1$: $f(x) = 4x^6 + 3x^5 + 30x^4 - 15x^3 + 45x^2 - 27x + 6$,
- $r = 2$: $f(x) = 6x^6 + 27x^5 + 45x^4 + 15x^3 + 30x^2 - 3x + 4$.

Acknowledgements

This material is based on private communications with Jens Franke, Joe Leherbauer, and Peter Montgomery.