Some problems in computational algebra.

Michael Monagan

Department of Mathematics, Simon Fraser University

November 2008

Outline

- Polynomial factorization over various fields,
- solving polynomial systems of equations,
- computing anti-derivatives and solutions of ODE and PDE $\times$

and

- rational number reconstruction, and
- computing heights of cyclotomic polynomials.

Polynomial factorization over finite fields.

Let $f(x)$ be a polynomial of degree n over GF(q) with k factors.

1967 E. Berlekamp. *Factoring polynomials over finite fields.*
[Bell System Technical Journal 46, 1967.]
Does $O(n^3 + kqn^2)$ arithmetic operations in $GF(q)$.

1981 D.G. Cantor and Hans Zassenhaus.
A Las Vegas algorithm: the expected number of arithmetic operations in GF(q) is $O(n^3 \log q)$.

1989 MBM implemented the C-Z algorithm in Maple.

1998 E. Kaltofen and V. Shoup. *Sub-quadratic time factoring of polynomials over finite field.* $\tilde{O}(n^{(\omega+1)/2} + n \log q)$ ops in GF(q) where n^ω is the cost of matrix-matrix multiplication.
Classical matrix-matrix multipliction: $\omega = 3$.
Best known $\omega = 2.376$ [D. Coppersmith and S. Winograd 1990.]

Polynomial factorization over finite fields.

Let $f(x)$ be a polynomial of degree n over GF(q) with k factors.

1967 E. Berlekamp. *Factoring polynomials over finite fields.*
[Bell System Technical Journal 46, 1967.]
Does $O(n^3 + kqn^2)$ arithmetic operations in $GF(q)$.

1981 D.G. Cantor and Hans Zassenhaus.
A Las Vegas algorithm: the expected number of arithmetic operations in GF(q) is $O(n^3 \log q)$.

1989 MBM implemented the C-Z algorithm in Maple.

1998 E. Kaltofen and V. Shoup. *Sub-quadratic time factoring of polynomials over finite field.* $\tilde{O}(n^{(\omega+1)/2} + n \log q)$ ops in GF(q) where n^ω is the cost of matrix-matrix multiplication.
Classical matrix-matrix multipliction: $\omega = 3$.
Best known $\omega = 2.376$ [D. Coppersmith and S. Winograd 1990.]

Polynomial factorization over finite fields.

Let $f(x)$ be a polynomial of degree n over $\mathrm{GF}(q)$ with k factors.

1967 E. Berlekamp. *Factoring polynomials over finite fields.*
[Bell System Technical Journal 46, 1967.]
Does $O(n^3 + kqn^2)$ arithmetic operations in $GF(q)$.

1981 D.G. Cantor and Hans Zassenhaus.
A Las Vegas algorithm: the expected number of arithmetic operations in $\mathrm{GF}(q)$ is $O(n^3 \log q)$.

1989 MBM implemented the C-Z algorithm in Maple.

1998 E. Kaltofen and V. Shoup. *Sub-quadratic time factoring of polynomials over finite field.* $\tilde{O}(n^{(\omega+1)/2} + n\log q)$ ops in $\mathrm{GF}(q)$ where n^ω is the cost of matrix-matrix multiplication.
Classical matrix-matrix multipliction: $\omega = 3$.
Best known $\omega = 2.376$ [D. Coppersmith and S. Winograd 1990.]

Polynomial factorization over finite fields.

Let $f(x)$ be a polynomial of degree n over $\mathrm{GF}(q)$ with k factors.

1967 E. Berlekamp. *Factoring polynomials over finite fields.*
[Bell System Technical Journal 46, 1967.]
Does $O(n^3 + kqn^2)$ arithmetic operations in $GF(q)$.

1981 D.G. Cantor and Hans Zassenhaus.
A Las Vegas algorithm: the expected number of arithmetic operations in $\mathrm{GF}(q)$ is $O(n^3 \log q)$.

1989 MBM implemented the C-Z algorithm in Maple.

1998 E. Kaltofen and V. Shoup. *Sub-quadratic time factoring of polynomials over finite field.* $\tilde{O}(n^{(\omega+1)/2} + n \log q)$ ops in $\mathrm{GF}(q)$
where n^ω is the cost of matrix-matrix multiplication.
Classical matrix-matrix multipliction: $\omega = 3$.
Best known $\omega = 2.376$ [D. Coppersmith and S. Winograd 1990.]

The Cantor-Zassenhaus algorithm.

Fermat's little theorem: if $a \in GF(q)$, $a \neq 0$ then $a^{q-1} = 1$.

$$\Rightarrow a^q = a \Rightarrow x^q - x = \prod_{a \in GF(q)} (x - a).$$

$$\Rightarrow \gcd(x^q - x, f(x)) = h(x)??$$

$$\Rightarrow \gcd(x^{q^2} - x, f(x)) =??$$

Now if q is odd then

$$x^q - x = x\,(x^{(q-1)/2} - 1)\underbrace{(x^{(q-1)/2} + 1)}_{??}$$

thus Pick $a \in GF(q)$ at random and compute

$$g = \gcd((x+a)^{(q-1)/2} + 1, h(x))$$

until $g \neq 1$ and $g \neq h$.

- Known to Gauss (for linear factors).

The Cantor-Zassenhaus algorithm.

Fermat's little theorem: if $a \in GF(q)$, $a \neq 0$ then $a^{q-1} = 1$.

$$\Rightarrow a^q = a \Rightarrow x^q - x = \prod_{a \in GF(q)} (x - a).$$

$$\Rightarrow \gcd(x^q - x, f(x)) = h(x)??$$

$$\Rightarrow \gcd(x^{q^2} - x, f(x)) = ??$$

Now if q is odd then

$$x^q - x = x\left(x^{(q-1)/2} - 1\right)\underbrace{\left(x^{(q-1)/2} + 1\right)}_{??}$$

thus Pick $a \in GF(q)$ at random and compute

$$g = \gcd((x + a)^{(q-1)/2} + 1, h(x))$$

until $g \neq 1$ and $g \neq h$.

- Known to Gauss (for linear factors).

The Cantor-Zassenhaus algorithm.

Fermat's little theorem: if $a \in GF(q)$, $a \neq 0$ then $a^{q-1} = 1$.

$$\Rightarrow a^q = a \Rightarrow x^q - x = \prod_{a \in GF(q)} (x - a).$$

$$\Rightarrow \gcd(x^q - x, f(x)) = h(x)??$$

$$\Rightarrow \gcd(x^{q^2} - x, f(x)) = ??$$

Now if q is odd then

$$x^q - x = x\,(x^{(q-1)/2} - 1)\underbrace{(x^{(q-1)/2} + 1)}_{??}$$

thus Pick $a \in GF(q)$ at random and compute

$$g = \gcd((x + a)^{(q-1)/2} + 1, h(x))$$

until $g \neq 1$ and $g \neq h$.

- Known to Gauss (for linear factors).

The Cantor-Zassenhaus algorithm.

Fermat's little theorem: if $a \in GF(q)$, $a \neq 0$ then $a^{q-1} = 1$.

$$\Rightarrow a^q = a \Rightarrow x^q - x = \prod_{a \in GF(q)} (x - a).$$

$$\Rightarrow \gcd(x^q - x, f(x)) = h(x)??$$

$$\Rightarrow \gcd(x^{q^2} - x, f(x)) =??$$

Now if q is odd then

$$x^q - x = x\,(x^{(q-1)/2} - 1)\underbrace{(x^{(q-1)/2} + 1)}_{??}$$

thus Pick $a \in GF(q)$ at random and compute

$$g = \gcd((x+a)^{(q-1)/2} + 1, h(x))$$

until $g \neq 1$ and $g \neq h$.

- Known to Gauss (for linear factors).

The Cantor-Zassenhaus algorithm.

Fermat's little theorem: if $a \in GF(q)$, $a \neq 0$ then $a^{q-1} = 1$.

$$\Rightarrow a^q = a \Rightarrow x^q - x = \prod_{a \in GF(q)} (x - a).$$

$$\Rightarrow \gcd(x^q - x, f(x)) = h(x)??$$

$$\Rightarrow \gcd(x^{q^2} - x, f(x)) = ??$$

Now if q is odd then

$$x^q - x = x\,(x^{(q-1)/2} - 1)\underbrace{(x^{(q-1)/2} + 1)}_{??}$$

thus Pick $a \in GF(q)$ at random and compute

$$g = \gcd((x + a)^{(q-1)/2} + 1, h(x))$$

until $g \neq 1$ and $g \neq h$.

- Known to Gauss (for linear factors).

The Cantor-Zassenhaus algorithm.

Fermat's little theorem: if $a \in GF(q)$, $a \neq 0$ then $a^{q-1} = 1$.

$$\Rightarrow a^q = a \Rightarrow x^q - x = \prod_{a \in GF(q)} (x - a).$$

$$\Rightarrow \gcd(x^q - x, f(x)) = h(x)??$$

$$\Rightarrow \gcd(x^{q^2} - x, f(x)) =??$$

Now if q is odd then

$$x^q - x = x\,(x^{(q-1)/2} - 1)\underbrace{(x^{(q-1)/2} + 1)}_{??}$$

thus Pick $a \in GF(q)$ at random and compute

$$g = \gcd((x+a)^{(q-1)/2} + 1, h(x))$$

until $g \neq 1$ and $g \neq h$.

- Known to Gauss (for linear factors).

Polynomial factorization over the rationals.

1969 Hans Zassenhaus. *On Hensel Factorization I.*

Hensel's Lemma: Suppose

$$f(x) \equiv \prod_{i=1}^{k} g_i(x) \pmod{p}.$$

If there are no repeated factors then for all $L \in \mathbb{N}$ there exist $h_i \in \mathbb{Z}[x]$ s.t. $h_i(x) \equiv g_i(x) \pmod{p}$ and

$$f(x) \equiv \prod_{i=1}^{k} h_i(x) \pmod{p^L}.$$

The Berlekamp-Hensel procedure (used by all CAS).
Step 1: Factor $f(x)$ over $\mathbb{Z}_p$.
Step 2: Hensel lift: compute the $h_i(x)$ mod $p^2, p^3, \ldots$
Step 3: Obtain factors of $f(x)$ from combinations of the $h_i(x)$.
Stop when p^L exceeds a coefficient bound on the factors of $f(x)$.

2002 Mark van Hoeij *Factoring Polynomials and the Knapsack Problem.*

Uses LLL to solve the combinatorial search in polynomial time.
Implemented by Mark in Maple in 2002.

Polynomial factorization over the rationals.

1969 Hans Zassenhaus. *On Hensel Factorization I.*

Hensel's Lemma: Suppose

$$f(x) \equiv \prod_{i=1}^{k} g_i(x) \pmod{p}.$$

If there are no repeated factors then for all $L \in \mathbb{N}$ there exist $h_i \in \mathbb{Z}[x]$ s.t. $h_i(x) \equiv g_i(x) \pmod{p}$ and

$$f(x) \equiv \prod_{i=1}^{k} h_i(x) \pmod{p^L}.$$

The Berlekamp-Hensel procedure (used by all CAS).
Step 1: Factor $f(x)$ over $\mathbb{Z}_p$.
Step 2: Hensel lift: compute the $h_i(x)$ mod $p^2, p^3, \ldots$
Step 3: Obtain factors of $f(x)$ from combinations of the $h_i(x)$.
Stop when p^L exceeds a coefficient bound on the factors of $f(x)$.

2002 Mark van Hoeij *Factoring Polynomials and the Knapsack Problem.*

Uses LLL to solve the combinatorial search in polynomial time.
Implemented by Mark in Maple in 2002.

Polynomial factorization over the rationals.

1969 Hans Zassenhaus. *On Hensel Factorization I.*

Hensel's Lemma: Suppose

$$f(x) \equiv \prod_{i=1}^{k} g_i(x) \pmod{p}.$$

If there are no repeated factors then for all $L \in \mathbb{N}$ there exist $h_i \in \mathbb{Z}[x]$ s.t. $h_i(x) \equiv g_i(x) \pmod{p}$ and

$$f(x) \equiv \prod_{i=1}^{k} h_i(x) \pmod{p^L}.$$

The Berlekamp-Hensel procedure (used by all CAS).
Step 1: Factor $f(x)$ over $\mathbb{Z}_p$.
Step 2: Hensel lift: compute the $h_i(x)$ mod $p^2, p^3, \ldots$
Step 3: Obtain factors of $f(x)$ from combinations of the $h_i(x)$.
Stop when p^L exceeds a coefficient bound on the factors of $f(x)$.

2002 Mark van Hoeij *Factoring Polynomials and the Knapsack Problem.*

Uses LLL to solve the combinatorial search in polynomial time.
Implemented by Mark in Maple in 2002.

Polynomial factorization over number fields.

1976 Barry Trager. *Algebraic factoring and rational function integration.*
To factor $f \in \mathbb{Q}(\alpha)[x]$ first factor $||f|| \in \mathbb{Q}[x]$.
Lemma: $f = \prod f_i \iff ||f|| = \prod ||f_i||$.
Then $\gcd(f, ||f_i||)$ is a factor of f.

2008 Ilias Kotsireas. Please factor

$$p = 19/2\, {c_4}^2 - \sqrt{11}\sqrt{5}\sqrt{2} c_5 c_4 - 2\sqrt{5} c_1 c_2 - 6\sqrt{2} c_3 c_4 + 7/2\, {c_1}^2 - \sqrt{7}\sqrt{3}\sqrt{2} c_3 c_2$$

$$+11/2\, {c_2}^2 - \sqrt{3}\sqrt{2} c_0 c_1 + 3/2\, {c_0}^2 + 23/2\, {c_5}^2 + 15/2\, {c_3}^2 - \frac{10681741}{1985}$$

- $||p|| \in \mathbb{Q}[c_0, c_1, \ldots, c_5]$ has over 3 million terms. DEMO

Polynomial factorization over number fields.

1976 Barry Trager. *Algebraic factoring and rational function integration.*
To factor $f \in \mathbb{Q}(\alpha)[x]$ first factor $||f|| \in \mathbb{Q}[x]$.
Lemma: $f = \prod f_i \iff ||f|| = \prod ||f_i||$.
Then $\gcd(f, ||f_i||)$ is a factor of f.

2008 Ilias Kotsireas. Please factor

$$p = 19/2\, {c_4}^2 - \sqrt{11}\sqrt{5}\sqrt{2} c_5 c_4 - 2\sqrt{5} c_1 c_2 - 6\sqrt{2} c_3 c_4 + 7/2\, {c_1}^2 - \sqrt{7}\sqrt{3}\sqrt{2} c_3 c_2$$

$$+11/2\, {c_2}^2 - \sqrt{3}\sqrt{2} c_0 c_1 + 3/2\, {c_0}^2 + 23/2\, {c_5}^2 + 15/2\, {c_3}^2 - \frac{10681741}{1985}$$

- $||p|| \in \mathbb{Q}[c_0, c_1, ..., c_5]$ has over 3 million terms. DEMO

Rational Number Reconstruction

Let $a = n/d$ where $\gcd(n, d) = 1$ and $d > 0$.
Let $u = a \bmod m$ where $\gcd(m, d) = 1$.
Given u and m find n/d.

The EEA(m,u) computes a sequence s_i, t_i, r_i satisfying

$$s_i m + t_i u = r_i \quad \text{for} \quad i = 0, 1, ..., k + 1.$$

Thus

$$r_i/t_i \equiv u \pmod{m} \;\; \text{if } \gcd(t_i, m) = 1.$$

Lemma (Wang 1981): if $m > 2|nd|$ then $n/d = r_j/t_j$ for some j.
Which rational r_i/t_i do we select?

Rational Number Reconstruction

Let $a = n/d$ where $\gcd(n, d) = 1$ and $d > 0$.
Let $u = a \bmod m$ where $\gcd(m, d) = 1$.
Given u and m find n/d.

The EEA(m,u) computes a sequence s_i, t_i, r_i satisfying

$$s_i m + t_i u = r_i \quad \text{for} \quad i = 0, 1, ..., k + 1.$$

Thus

$$r_i/t_i \equiv u \pmod{m} \;\; \text{if} \; \gcd(t_i, m) = 1.$$

Lemma (Wang 1981): if $m > 2|nd|$ then $n/d = r_j/t_j$ for some j.
Which rational r_i/t_i do we select?

Rational Number Reconstruction

Let $a = n/d$ where $\gcd(n, d) = 1$ and $d > 0$.
Let $u = a \bmod m$ where $\gcd(m, d) = 1$.
Given u and m find n/d.

The EEA(m,u) computes a sequence s_i, t_i, r_i satisfying

$$s_i m + t_i u = r_i \quad \text{for} \quad i = 0, 1, ..., k + 1.$$

Thus

$$r_i/t_i \equiv u \pmod{m} \;\; \text{if } \gcd(t_i, m) = 1.$$

Lemma (Wang 1981): if $m > 2|nd|$ then $n/d = r_j/t_j$ for some j.
Which rational r_i/t_i do we select?

Rational Number Reconstruction

$n/d = 72/109$, $m = 999987$, $u = 137613$, $m/|2nd| = 63.7$

i	r_i	t_i	q_{i+1}	r_i/t_i
1	137613	1	7	$\frac{137613}{1}$
2	36692	-7	3	$\frac{-36692}{7}$
3	27537	22	1	$\frac{27537}{22}$
4	9155	-29	3	$\frac{-9155}{29}$
5	72	109	127	$\frac{72}{109}$
6	11	-13872	6	$\frac{-11}{13872}$
7	6	83341	1	$\frac{6}{83341}$
8	5	-97213	1	$\frac{-5}{97213}$
9	1	180554	5	$\frac{1}{180554}$

Table: Output from EEA($m = 10^6 - 17$, $u = 137613$).

Lemma (i) $m/3 \leq q_{i+1}|r_i t_i| \leq m$, (ii) $1 \leq \prod q_i \leq m$ and

(iii) Over all inputs $0 \leq u < m$, $\mathrm{E}[q_i] \in O(\log m)$.

$\Longrightarrow$ accept r_i/t_i if $q_{i+1} > 2^k(\log m)$.

Rational Number Reconstruction

$n/d = 72/109,\ m = 999987,\ u = 137613,\ m/|2nd| = 63.7$

i	r_i	t_i	q_{i+1}	r_i/t_i
1	137613	1	7	$\frac{137613}{1}$
2	36692	-7	3	$\frac{-36692}{7}$
3	27537	22	1	$\frac{27537}{22}$
4	9155	-29	3	$\frac{-9155}{29}$
5	72	109	127	$\frac{72}{109}$
6	11	-13872	6	$\frac{-11}{13872}$
7	6	83341	1	$\frac{6}{83341}$
8	5	-97213	1	$\frac{-5}{97213}$
9	1	180554	5	$\frac{1}{180554}$

Table: Output from EEA($m = 10^6 - 17,\ u = 137613$).

Lemma (i) $m/3 \leq q_{i+1}|r_i t_i| \leq m$, (ii) $1 \leq \prod q_i \leq m$ and
(iii) Over all inputs $0 \leq u < m$, $E[q_i] \in O(\log m)$.
$\Longrightarrow$ accept r_i/t_i if $q_{i+1} > 2^k(\log m)$.

Gröbner Bases

1965 Bruno Buchberger. *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal,* Ph.D. thesis, University of Innsbruck.

Definition: Let $f_1, f_2, ..., f_s$ be polynomials in $k[x_1, x_2, ..., x_n]$ and $>$ be a monomial ordering. $G = \{g_1, g_2, ..., g_t\}$ is a Gröbner basis for the ideal $I = \langle f_1, f_2, ..., f_s \rangle$ wrt $>$ if

$$f \in I \textit{ iff the remainder of } f \div G \textit{ is } 0.$$

- The solutions of $\{f_1 = 0, ... f_s = 0\}$ equal those of $\{g_1 = 0, ..., g_t = 0\}$.
- Buchberger gave an algorithm for computing a Gröbner basis.

1999 Jean-Charles Faugere.

A new efficient algorithm for computing Gröbner bases (F4).

Roman Pearce incorporated his GB package into Maple 11.

Gröbner Bases

1965 Bruno Buchberger. *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal*, Ph.D. thesis, University of Innsbruck.

Definition: Let $f_1, f_2, ..., f_s$ be polynomials in $k[x_1, x_2, ..., x_n]$ and $>$ be a monomial ordering. $G = \{g_1, g_2, ..., g_t\}$ is a Gröbner basis for the ideal $I = \langle f_1, f_2, ..., f_s \rangle$ wrt $>$ if

$$f \in I \textit{ iff the remainder of } f \div G \textit{ is } 0.$$

- The solutions of $\{f_1 = 0, ... f_s = 0\}$ equal those of $\{g_1 = 0, ..., g_t = 0\}$.
- Buchberger gave an algorithm for computing a Gröbner basis.

1999 Jean-Charles Faugere. *A new efficient algorithm for computing Gröbner bases (F4).* Roman Pearce incorporated his GB package into Maple 11.

Gröbner Bases

1965 Bruno Buchberger. *An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal,* Ph.D. thesis, University of Innsbruck.

Definition: Let $f_1, f_2, ..., f_s$ be polynomials in $k[x_1, x_2, ..., x_n]$ and $>$ be a monomial ordering. $G = \{g_1, g_2, ..., g_t\}$ is a Gröbner basis for the ideal $I = \langle f_1, f_2, ..., f_s \rangle$ wrt $>$ if

$$f \in I \textit{ iff the remainder of } f \div G \textit{ is 0.}$$

- The solutions of $\{f_1 = 0, ... f_s = 0\}$ equal those of $\{g_1 = 0, ..., g_t = 0\}$.
- Buchberger gave an algorithm for computing a Gröbner basis.

1999 Jean-Charles Faugere.

A new efficient algorithm for computing Gröbner bases (F4).

Roman Pearce incorporated his GB package into Maple 11.

Triangular Sets

1950 J. Ritt. Ritt-Wu Characteristic Sets.

1978 rediscovered by W. Wu.

1991 Michael Kalkbrenner. Regular Chains

A generalized Euclidean algorithm for computing triangular representations of algebraic varieties.

2005 Implemented in Maple 11 by Marc Moreno Maza. DEMO

2004 Dahan and Schost. *Sharp estimates for triangular sets.*

Let $F = \{f_1, \dots, f_n\} \subset \mathbb{Z}[x_1, \dots, x_n]$ have degree $\leq d$.
Suppose $\{f_1 = 0, \dots, f_n = 0\}$ has at most d^n solutions over $\mathbb{C}$.
Let h bound the size of the largest integer in F.
Then the length of the integers in G is bounded by (essentially) $nh(d^n)^2$.
Moreover the length of the integers in T is bounded by nhd^n.

Triangular Sets

1950 J. Ritt. Ritt-Wu Characteristic Sets.

1978 rediscovered by W. Wu.

1991 Michael Kalkbrenner. Regular Chains

A generalized Euclidean algorithm for computing triangular representations of algebraic varieties.

2005 Implemented in Maple 11 by Marc Moreno Maza. DEMO

2004 Dahan and Schost. *Sharp estimates for triangular sets.*

Let $F = \{f_1, ..., f_n\} \subset \mathbb{Z}[x_1, ..., x_n]$ have degree $\leq d$.

Suppose $\{f_1 = 0, ..., f_n = 0\}$ has at most d^n solutions over $\mathbb{C}$.

Let h bound the size of the largest integer in F.

Then the length of the integers in G is bounded by (essentially) $nh(d^n)^2$.

Moreover the length of the integers in T is bounded by nhd^n.

Triangular Sets

1950 J. Ritt. Ritt-Wu Characteristic Sets.

1978 rediscovered by W. Wu.

1991 Michael Kalkbrenner. Regular Chains

A generalized Euclidean algorithm for computing triangular representations of algebraic varieties.

2005 Implemented in Maple 11 by Marc Moreno Maza. DEMO

2004 Dahan and Schost. *Sharp estimates for triangular sets.*
Let $F = \{f_1, ..., f_n\} \subset \mathbb{Z}[x_1, ..., x_n]$ have degree $\leq d$.
Suppose $\{f_1 = 0, ..., f_n = 0\}$ has at most d^n solutions over $\mathbb{C}$.
Let h bound the size of the largest integer in F.
Then the length of the integers in G is bounded by (essentially) $nh(d^n)^2$.
Moreover the length of the integers in T is bounded by nhd^n.

Cyclotomic Polynomials

The n'th cyclotomic polynomial $\Phi_n(x)$ is the irreducible factor of $x^n - 1$ whose roots are the primitive n'th roots of unity.

n	$\Phi_n(x)$
3	$x^2 + x + 1$
4	$x^2 + 1$
5	$x^4 + x^3 + x^2 + x + 1$
6	$x^2 - x + 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$x^4 + 1$
9	$x^6 + x^3 + 1$
10	$x^4 - x^3 + x^2 - x + 1$

cyclotomic polynomials of order 3–10

Cyclotomic Polynomials

$$\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36}$$
$$+ \ldots + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - \mathbf{2}x^{7} - x^{6} - x^{5} + x^{2} + x + 1.$$

$$\Phi_{385}(x) = x^{240} + x^{239} + x^{238} + x^{237} + x^{236} - x^{233} - x^{232} - x^{231} - x^{230} - 2\,x^{229}$$
$$- \ldots - 2\,x^{122} - 3\,x^{121} - \mathbf{3}\,x^{120} - \mathbf{3}\,x^{119} - 2\,x^{118} - 2\,x^{117} - x^{116} + \ldots + x + 1$$

Cyclotomic Polynomials

n	H_n	n	H_n
105	2	26565	59
385	3	40755	359
1365	4	106743	397
1785	5	171717	434
2805	6	255255	532
3135	7	279565	585
6545	9	285285	1182
10465	14	327845	31010
11305	23	707455	35111
17255	25	886445	44125
20615	27	983535	59518

H_n is the biggest coefficient in $\Phi_n(x)$.

Very Large Heights

1998 Koshiba Yoichi $H_{4849845} = 669606$ where

$n = 4849845 = (3)(5)(7)(11)(13)(17)(19)$

1974 Paul Erdos

For any $c > 0$ there exists n such that $H_n > n^c$.

n	H_n
$1181895 = (3)(5)(11)(13)(19)(29)$	$14102773 > n^1$ (MBM)
$43730115 = (3)(5)(11)(13)(19)(29)(37)$	$862550638890874931 > n^2$ (MBM)
$416690995 = (5)(7)(17)(19)(29)(31)(41)$	$80103182105128365570406901971 > n^3$ (AA)
$1880394945 = (3)(5)(11)(13)(19)(29)(37)(43)$	$64540997036010911566826446181523888971563 > n^4$ (AA).

Very Large Heights

1998 Koshiba Yoichi $H_{4849845} = 669606$ where

$n = 4849845 = (3)(5)(7)(11)(13)(17)(19)$

1974 Paul Erdos

For any $c > 0$ there exists n such that $H_n > n^c$.

n	H_n
$1181895 = (3)(5)(11)(13)(19)(29)$	$14102773 > n^1$ (MBM)
$43730115 = (3)(5)(11)(13)(19)(29)(37)$	$862550638890874931 > n^2$ (MBM)
$416690995 = (5)(7)(17)(19)(29)(31)(41)$	$80103182105128365570406901971 > n^3$ (AA)
$1880394945 = (3)(5)(11)(13)(19)(29)(37)(43)$	$6454099703601091156682644618152388897156 3 > n^4$ (AA).

Computing $\Phi_n(x)$ via sparse power series.

$$\Phi_{15}(x) = \frac{(1-x^{15})(1-x)}{(1-x^3)(1-x^5)} = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8.$$

Let n be a product of k distinct primes. The general formula has 2^k multiplications and 2^k divisions each of which can computed in $O(n)$ integer additions.

Thank you.