Who was Who in polynomial factorization

Joachim von zur Gathen
b-it
Universität Bonn
D-53113 Bonn
gathen@bit.uni-bonn.de

Categories and Subject Descriptors: I.1.0 [Symbolic and algebraic manipulation]: Algorithms.

General Terms: Algorithms.

Keywords: Polynomial factorization, history.

This invited talk presents some developments in the history of factoring polynomials. We restrict our discussion to univariate polynomials over the integers or the integers modulo a prime, and do not strive for completeness.

In the beginning was root-finding. The Babylonians had numerical algorithms for solving quadratic equations, around 1900–1600 BC. Somewhat later, they also solved cubic equations of the form $ax^3 + bx^2 = c$ numerically, and had mastered quadratics symbolically. For example, to solve

$$x + \frac{1}{x} = a,$$

they compute

$$b = (\frac{a}{2})^2,$$
$$r = \sqrt{b-1},$$
$$x_{1,2} = \frac{a}{2} \pm r.$$

Of course, they had no way of thinking in terms of such equations, but the cuneiform clay tablets explain the algorithm for some specific values of a.

For the next millenia, no essential progress happened. Finally, Renaissance enlightenment dispelled the medieval clouds from European minds, and Italian mathematicians found the symbolic solutions for cubic and quartic equations. First, Scipione del Ferro (c.1465–1526) and Nicolò Tartiaglia (c.1500–1557) for degree 3, published by Geronimo Cardano (1501–1576) in his *Ars Magna*; a cloak-and-dagger story of betrayal and disregard for intellectual property rights.

François Viète (1540–1603) discovered the relation between roots and coefficients of a polynomial, Pierre Fermat (1601–1665) his "Little Theorem" which we write today as the symbolic factorization

$$x^p - x = \prod_{a \in \mathbb{Z}_p} (x - a) \qquad (1)$$

for a prime p, and Isaac Newton (1642–1727) his method for approximating real roots of a polynomial.

ISSAC'06, July 9–12, 2006, Genova, Italy.

Figure 1: Adrien Marie Legendre

At the end of the 18th century, two ideas were proposed that lie at the heart of modern factorization algorithms over finite fields, but were forgotten and rediscovered a century and a half later.

The first is Adrien Marie Legendre's (1752–1833) method for finding the roots of $f \in \mathbb{Z}_p[x]$, for an odd prime p. He factors (1) symbolically as

$$x^p - x = x \cdot (x^{(p-1)/2} - 1) \cdot (x^{(p-1)/2} + 1)$$

and observes that the gcd of f with each of the two latter factors splits the (nonzero) roots of f into two sets (namely the squares and the nonsquares). Now comes an amazing proposal: you replace x by $x+a$ for random a and continue to split the partial factorization. This is the mother of all probabilistic algorithms, and it is still the most efficient approach we know for this problem today!

Next came one of the towering giants of mathematics, Carl Fried-

Figure 2: Carl Friedrich Gauß

rich Gauß (1777–1855). His contributions to symbolic factorization include:

- $R[x]$ is a Unique Factorization Domain if R is,
- primitive polynomials, factoring in $\mathbb{Z}[x]$ vs. in $\mathbb{Q}[x]$,
- Gaußian elimination for linear equations,
- p-adic lifting,
- rudiments of basis reduction in lattices,
- computing the squarefree part,
- distinct-degree factorization.

Gauß had been led to the latter by his experimental discovery of the Prime Number Theorem. For an analogue in $\mathbb{F}_p[x]$, he generalized (1) as

$$x^{p^d} - x = \prod g,$$

where the product is over those irreducible monic $g \in \mathbb{Z}_p[x]$ whose degree divides d. He used this to determine the number of irreducible polynomials of degree d. Gauß also specified the algorithm of iteratively taking the gcd of f with $x^p - 1, x^{p^2} - 1, \ldots$ and removing each factor found. This *distinct-degree factorization* splits f into factors all of whose irreducible factors have the same degree. It is a staple of modern factorization algorithms. This material was meant to be included in the eighth chapter of his *Disquisitiones Arithmeticae*, written in 1798 and 1799. A generous grant by the Duke of Brunswick financed its publication in 1801. This work was to shape number theory for decades. But publishing mathematical books was a risky venture, and the Duke's money only stretched to seven chapters. So the factorization ideas disappeared in Gauß' stack of papers and were only published posthumously, in 1863. This was in Latin and left to later computer algebraists the joy of rediscovering Gauß' methods, unfettered by historical precedents. David Cantor and Hans Zassenhaus (1912–1991) introduced distinct-degree factorization into modern computer algebra.

For factoring in $\mathbb{Z}[x]$, no algorithm is obvious as long as the coefficients of factors are not bounded. Leopold Kronecker (1823–1891) gave a simple approach in 1882: evaluate at sufficiently many integer points, factor the integer values and try the interpolating polynomials through all possible factor combinations. This is indeed an algorithm, but impractical. Newton had suggested this method, with divided differences for interpolation, for linear and quadratic factors. This was generalized by Friedrich Theodor von Schubert in 1793 and later by Joseph Diaz Gergonne (1771–1859).

The next two major contributions have survived to this day: integer lattices introduced in Hermann Minkowski's (1864–1909) *geometry of numbers*, and Kurt Hensel's (1861–1941) p-adic approach. His procedure now called *Hensel lifting* allows to lift a modular factorization $f \equiv g \cdot h \bmod p$, with $f, g, h \in \mathbb{Z}[x]$ and g and h coprime modulo the prime p, to a (unique) factorization $f \equiv g^* \cdot h^*$ modulo p^k for any $k \geq 2$, with $g^* \equiv g$, $h^* \equiv h \bmod p$. Like so many things, this is already in Gauß' notes.

There are some more ingredients to modern factorization algorithms. The most important one started with the discovery in Arjen Lenstra's (*1956) PhD thesis of a connection between short vectors in a certain integer lattice and polynomial factors in $\mathbb{Z}[x]$. In their landmark 1982 paper, Arjen and Hendrik Lenstra (*1949) and László Lovász (*1948) described a polynomial-time computation for such short vectors. This has found application in many areas, transcending its original goal of polynomial-time factorization of polynomials in $\mathbb{Q}[x]$. A second ingredient is an a priori bound on factors of integer polynomials, going back to Maurice Mignotte in 1974. A third one is a different approach to factoring in $\mathbb{Z}_p[x]$, using linear algebra. This was proposed by Elwyn Berlekamp (*1940) in 1970, using a matrix that had been studied by Karel Petr, Štefan Švarc (Schwarz, 1914–1996), and Michael Butler. This algorithm also has the distinction of being the first modern polynomial-time probabilistic algorithm. This use of randomness in computation is now accepted as an important tool, but its relevance was not recognized at the time, until the probabilistic primality test of Robert Solovay (*1938) and Volker Strassen (*1936).

Finally, for the factorization of large polynomials, say of degree one million over $\mathbb{Z}_2$, one has to improve Gauß' distinct-degree factorization in two ways: the various x^{p^d} are calculated not by exponentiation but by modular composition, with a method due to Richard Brent (*1946) and one must arrange to take a gcd not for each individual value of d, but for many at a time. This was developed in the 1990s and is sometimes called the "von zur Gathen-Kaltofen-Shoup method".

In summary, the basic polynomial factorization technology in, say, 1990, can be derived from the following sources:

- Gauß' methods,
- Legendre's probabilistic idea for linear factors,
- the latter's generalization to higher degrees,
- the short vector algorithm of Lenstra, Lenstra, Lovász.

The success story of polynomial factorization is unthinkable without computer algebra systems, pioneered by George Collins and many others from the 1960s on.