International Journal of Engineering & Technology, 7 (4.10) (2018) 112-117

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Factoring Polynomials Using Elliptic Curves

A. Uma Maheswari[1] and Prabha Durairaj[2]

Quaid-E-Millath Government College for Women (Autonomous)
Chennai - 600 002, India
**Corresponding author E-mail: 1umashiva2000@yahoo.com, 2prabhadurairaj59@gmail.com*

Abstract

This paper presents a probabilistic algorithm to factor polynomials over finite fields using elliptic curves. The success of the algorithm depends on the initial choice of elliptic curve parameters. The algorithm is illustrated through numerical examples.

Keywords*: Elliptic curve, polynomial factorization over finite fields, irreducible polynomial.*

1. Introduction

Factorization algorithms for polynomials over finite fields have applications in coding theory and in the study of linear recurrence relations in finite fields [1]. Many computational problems in Algebra and Number Theory like the Index Calculus Algorithm depend on the factorization of polynomials over finite fields [2,3]. A well-known algorithm to factor polynomials over finite fields is the Berlekamp Algorithm [4]. This is a deterministic procedure for reducing the problem of factoring an arbitrary polynomial over the Galois field $GF(p^m)$ to the problem of finding the roots in $GF(p)$ of certain other polynomials over $GF(p)$. Related algorithms on polynomial factoring are found in [5,6,7,8,9,10].

Elliptic curves over finite fields provide an inexhaustible supply of finite abelian groups and are amenable to computation because of their rich structure. H.W.Lenstra [11] made an ingenious use of elliptic curves and evolved a factorization method to factor composite integers. In this work, a new algorithm to factor polynomials over finite fields analogous to Lenstra's method has been devised.

This paper is structured as follows. Section 2 reviews the basic theory of elliptic curves over rings. In section 3 a new congruence relation is defined on the field of quotients of the polynomial ring $F_p[x]$; lemmas and theorems that form the basis for the new algorithm are proved, the new factoring algorithm is presented and illustrated with numerical examples followed by conclusion.

2. Preliminary Concepts:

This section presents an overview of the theory of elliptic curves over Rings.

Elliptic curves over Rings:[12]

For our purposes it is necessary to work with elliptic curves that are defined over Rings. The general theory of elliptic curves over commutative rings with 1 is discussed in [13]. We list down some basic definitions and results.

Let R be a commutative ring with 1 satisfying the following conditions:

i. $6 \in R^*$

ii. If (a_{ij}) is an mxn matrix such t $(a_{11}, a_{12}, \dots a_{mn})$ is primitive and such that all $2x2$ subdeterminants vanish (that is, $a_{ij}a_{kl} - a_{il}a_{kj} = 0$ for all i, j, k, l) then some R -linear combination of the rows is a primitive n -tuple.

An elliptic curve E over a ring R (satisfying conditions (i) and (ii)) is given by the homogeneous Weierstrass equation $y^2z = x^3 + Axz^2 + Bz^3$ with $A, B \in R$ such that $(4A^3 + 27B^2) \in R^*$. We define $E(R) = \{(x:y:z) \in P^2(R) / y^2z = x^3 + Axz^2 + Bz^3\}$, where $P^2(R)$ is the projective plane over R

The point $(0:1:0) \in E(R)$ is called the zero point of the curve and is denoted by O. The addition formulae and the proof that $E(R)$ is a group can be found in [14].

The affine equation of the elliptic over R is $y^2 = x^3 + Ax + B$

Theorem 2.1[15]:

Let E be an elliptic curve over Q given by, $y^2 = x^3 + Ax + B$, with $A, B \in Z$. Let n be a positive odd integer such that $gcd(n, 4A^3 + 27B^2) = 1$. Represent the elements of $E(Q)$ as primitive triples $(x:y:z) \in P^2(z)$.

The map $red_n : E(Q) \to E(Z_n)$, $(x:y:z) \mapsto (x:y:z)(\mathrm{mod}\, n)$ is a group homomorphism.

The above theorem can be generalized as follows:

Theorem 2.2[15]:
Let R be a ring and let I be an ideal of R. Assume that both R and R/I satisfy conditions (i) and (ii). Let E be given by $y^2z = x^3 + Axz^2 + Bz^3$ with $A, B \in R$ and assume there exists $r \in R$ such that $(4A^3 + 27B^2)r - 1 \in I$.

Then the map $red_n : E(R) \to E(R/I)$, $(x:y:z) \mapsto (x:y:z) \mathrm{m}od\ I$ is a group homomorphism.

3. New Factoring Algorithm

In this section a new algorithm for factoring polynomials over a finite field, using elliptic curves, is devised in line with Lenstra's algorithm [11]. New relations, related lemmas and theorems central to the algorithm are defined and proved.

In the following sequel, $F_p[x]$ is the ring of polynomials over the finite field F_p; $T(x)$ is its field of quotients (i.e) $T(x)$ is the field of rational functions formed with polynomials over F_p.

In analogy with the congruence relation defined on the set of rational numbers [16], we define a relation, "Congruence modulo a polynomial $h(x)$" on the field $T(x)$ as follows:

Definition 3.1:
For any polynomial $h(x) \in F_p[x]$ and any two rational functions $s(x), t(x)$ in $T(x)$ with denominators prime to $h(x)$ we write $s(x) \equiv t(x)(\mathrm{m}od\ h(x))$, if $(s(x) - t(x))$ written in lowest terms has numerator divisible by $h(x)$.

This is an equivalence relation on the field of rational functions $T(x)$.

Lemma 3.2:
For any rational function $s(x) \in T(x)$ with denominator prime to $h(x) \in F_p[x]$, there is a unique polynomial $y_0(x) \in F_p[x]$ such that $s(x) \equiv y_0(x)(\mathrm{m}od\ h(x))$.

Proof:
Let $s(x) = \frac{a(x)}{b(x)}$ where $a(x), b(x) \in F_p[x]$ and $gcd(b(x), h(x)) = 1$.

Consider the congruence $b(x)y(x) \equiv a(x) \mathrm{m}od\ h(x)$. Since $gcd(b(x), h(x)) = 1$ this congruence has a unique solution $y_0(x)$ given by, $y_0(x) = \left((b(x))^{-1} a(x) \bmod h(x)\right)$ where $b(x)$ is inverted using its extended gcd with $h(x)$. Thus $b(x)y_0(x) \equiv a(x) \mathrm{m}od\ h(x)$

This implies that $a(x) - b(x)y_0(x) = h(x) f(x)$ for some $f(x) \in F_p[x]$. Then $\frac{(a(x) - b(x)y_0(x))}{b(x)}$ when written in lowest terms, has numerator divisible by $h(x)$. (i.e) $\frac{a(x)}{b(x)} \equiv y_0(x)(\mathrm{m}od\ h(x))$ (or) $s(x) \equiv y_0(x)(\mathrm{m}od\ h(x))$ (degof $y_0(x) <$ degof $h(x)$)

Definition 3.3:

Let $s(x) \in T(x)$ be a rational function with denominator prime to a polynomial $h(x) \in F_p[x]$. If $s(x) = \frac{a(x)}{b(x)}$, where $a(x), b(x) \in F_p[x]$, then the polynomial $y_0(x) \in F_p(x)$ of lowest degree satisfying the congruence $b(x)y(x) \equiv a(x) \bmod h(x)$ is called the 'residue of $s(x)$ modulo $h(x)$'. We write $s(x) \bmod h(x) = y_0(x)$

Lemma 3.4:
For any two rational functions $X_1(x)$ and $X_2(x)$ in $T(x)$ with denominators prime to a polynomial $h(x) \in F_p[x]$, $X_1(x) \equiv X_2(x) \bmod h(x)$ iff $X_1(x) \bmod h(x) = X_2(x) \bmod h(x)$

Note:
Let us denote $X_1(x) = X_1, Y_1(x) = Y_1$ (for brevity's sake).

Proof:
Let $X_1 \equiv X_2 \bmod h(x)$. We shall show that $X_1 \bmod h(x) \equiv X_2 \bmod h(x)$

Let $X_1 = \frac{p_1(x)}{q_1(x)}$, $X_2 = \frac{p_2(x)}{q_2(x)}$ where $p_i(x), q_i(x) \in F_p[x]$ and $gcd(q_i(x), h(x)) = 1, i = 1,2.$

Then $X_1 - X_2$ when written in lowest terms has numerator divisible by h(x).

$$\frac{(p_1(x)q_2(x) - p_2(x)q_1(x))}{q_1(x)q_2(x)} = \frac{l(x)}{m(x)}\left(h(x)\right)^r \text{ where } r \geq 1 \qquad (3.1)$$

is chosen such that neither $l(x)$ nor $m(x)$ is divisible by $h(x)$.

$$\text{Let } X_1(x) \bmod h(x) = y_0(x) \text{ where } y_0(x) \in F_p[x] \qquad (3.2)$$

$$\text{Then } p_1(x) - q_1(x)y_0(x) \equiv 0 \bmod h(x) \qquad (3.3)$$

We shall show that $X_2 \bmod h(x)$ is also equal to $y_0(x)$. (i.e) $y_0(x)$ is the solution of the polynomial congruence $q_2(x)y(x) \equiv p_2(x) \bmod h(x)$

Multiplying (3.3) by $q_2(x)$ and using (3.1) we get,

$p_1(x)q_2(x) = p_2(x)q_1(x) + q_1(x)q_2(x)\frac{l(x)}{m(x)}\left(h(x)\right)^r$, which implies

$$\left(p_2(x) - y_0(x)q_2(x)\right)q_1(x) \equiv 0 \bmod h(x) \qquad (3.4)$$

since $gcd(q_1(x), h(x)) = 1$, we have,

$p_2(x) - y_0(x)q_2(x) \equiv 0 \bmod h(x)$.(i.e) $y_0(x)$ is the solution of the congruence $p_2(x) \equiv y(x)q_2(x) \bmod h(x)$

$$X_2 \bmod h(x) = y_0(x) \qquad (3.5)$$

From (3.2) and (3.5), we conclude that $X_1 \bmod h(x) = X_2 \bmod h(x)$

Conversely, Suppose $X_1 \bmod h(x) = X_2 \bmod h(x) = y_0(x)$ where $y_0(x) \in F_p[x]$.

Then $q_1(x)y_0(x) - p_1(x) = r_1(x)h(x)$ forsome $r_1(x) \in F_p[x]$ (3.6)

and $q_2(x)y_0(x) - p_2(x) = r_2(x)h(x)$ forsome $r_2(x) \in F_p[x]$ (3.7)

Multiplying (3.6) by $q_2(x)$ and (3.7) by $q_1(x)$ and subtracting, we get

$$\frac{p_1(x)q_2(x) - p_2(x)q_1(x)}{q_1(x)q_2(x)}$$
$$= h(x)\frac{\left(r_2(x)q_1(x) - r_1(x)q_2(x)\right)}{q_1(x)q_2(x)}$$

Observe that $gcd(q_i(x), h(x)) = 1, i = 1,2.$ $(3.8) \Rightarrow X_1 - X_2$ when written in lowest terms has numerator divisible by $h(x)$

$$\therefore X_1 \equiv X_2 \bmod h(x)$$

Elliptic Curves - Reduction Modulo $f(x)$

Let $f(x) \in F_p(x)$ be a polynomial whose factorization is required; Let R denote the Residue class ring $\dfrac{F_p[x]}{(f(x))}$. This is a finite ring satisfying conditions (i) and (ii). For polynomials $A, B \in R$ consider the elliptic curve over R, $Y^2 = X^3 + AX = B$, denoted by $E(R)$. $E(R)$ consists of pairs $(X,Y) \in (RXR)$ which satisfy the above equation together with a point at infinity O. On this set we define, (as we defined for curves over fields) an addition that we call partial addition. (i.e) We define $P + O = O + P = P$ for all P in E. The partial inverse $-P$ of a point $P = (X,Y)$ is $-P = (X,-Y)$.

If $P, Q \in E(R) - O$, with $P = (X_1, Y_1)$, $Q = (X_2, Y_2)$.

$$\text{weset}\lambda = \begin{cases} (Y_2 - Y_1)/(X_2 - X_1) & \text{if } P \neq Q \\ (3X_1^2 + A)/2Y_1 & \text{if } P = Q. \end{cases}$$

and $X_3 = \lambda^2 - X_1 - X_2$ and define $P + Q = (X_3, \lambda(X_1 - X_3) - Y_1)$. Here calculations are performed modulo $f(x)$ and modulo p. Thus if $P \neq Q$,

$$P + Q = (X_3, Y_3) = \left(\begin{array}{l} \left(\left(\dfrac{Y_2 - Y_1}{X_2 - X_1} \right)^2 - X_1 - X_2 \right), \\ \left(-Y_1 + \left(\dfrac{Y_2 - Y_1}{X_2 - X_1} \right)(X_1 - X_3) \right) \end{array} \right)$$

If $P = Q,\ 2P = (X_3, Y_3)$

$$= \left(\begin{array}{l} \left(\left(\dfrac{3X_1^2 + A}{2Y_1} \right)^2 - X_1 - X_2 \right), \\ \left(-Y_1 + \left(\dfrac{3X_1^2 + A}{2Y_1} \right)(X_1 - X_3) \right) \end{array} \right) \qquad (3.10)$$

Since in $R = \dfrac{F_p[x]}{(f(x))}$ there exist zero divisors that may appear as denominators in these formulas, the composition law may fail to add points. (that is why it is called a partial addition). When we add two points or double a point the possibilities are: (i) we get a well defined point because the denominator of the slope is invertible modulo $f(x)$ (ii) if the points are of the form (X,Y) and $(X,-Y)$ then we get the point at infinity (iii) we get an undefined point because the denominator of the slope λ is a multiple of p; hence it is neither zero mod $f(x)$ nor invertible (iv) denominator of slope λ is not invertible mod $f(x)$ because its extended gcd with $f(x)$ is not one or $f(x)$ but gives a non trivial divisor of $f(x)$. So one has to detect this fact in the modular inversion routine and obtain a divisor of $f(x)$.

To find an irreducible factor of a polynomial $f(x) \in F_p[x]$ using the Elliptic Curve Method.

Suppose an elliptic curve $E(R)$ and a point $P = (X,Y)$ on it are chosen in some 'random' way. We want to find the multiple kP for a suitable positive integer k. We shall consider the point P and all its multiples modulo $f(x)$ (using the repeated doubling method.) We let $P \bmod f(x) = (X \bmod f(x), Y \bmod f(x))$ and every time we compute some multiple kP, we compute only the reduction of the co-ordinates modulo *f(x)*. In order to be able to work modulo $f(x)$, there is a non-trivial condition that must hold good when we add two different points. (i.e) All denominators must be prime to $f(x)$.

The following theorem proves that when we encounter a denominator that is not prime to $f(x)$, the gcd of that denominator with $f(x)$ yields a proper divisor of $f(x)$.

Proposition 3.4:

Let E be an elliptic curve over the field of rational functions $T(x)$ with equation $Y^2 = X^3 + AX + B$ where $A, B \in F_p[x]$ and $gcd(4A^3 + 27B^2, f(x)) = 1$. Let P_1 and P_2 be two points on E whose coordinates have denominators prime to $f(x)$ where $P_1 \neq -P_2$. Then $(P_1 + P_2) \in E$ has co-ordinates with denominators prime to $f(x)$ iff there is no irreducible polynomial $m(x) \mid f(x)$ (where $m(x)$ is irreducible over F_p) with the following property: The points $P_1 \bmod m(x)$ and $P_2 \bmod m(x)$ on the elliptic curve $E \bmod m(x)$ add up to the point at infinity $O \bmod m(x) \in E \bmod m(x)$. Here $E \bmod m(x)$ denotes the elliptic curve over $F_{m(x)}$ obtained by reducing modulo $m(x)$ the coefficients of the equation $Y^2 = X^3 + AX + B$. ($F_{m(x)}$ denotes $\dfrac{F_p[x]}{(m(x))}$, the field of residue classes modulo $m(x)$).

Proof:

The elliptic curve $E = \{(X,Y)/Y^2 = X^3 + AX + B,\ A, B \in F_p[x]\}$.

Let $P_1 = (X_1, Y_1),\ P_2 = (X_2, Y_2)$ and $P_1 + P_2$ have co-ordinates with denominators prime to $f(x)$.

Let $m(x)$ be any irreducible factor of $f(x)$ (irreducible over F_p). We shall show that $P_1 \bmod m(x) + P_2 \bmod m(x) \neq O \bmod m(x)$.

Case(i): Suppose $X_1 \not\equiv X_2 \bmod m(x)$

Now $P_1 \bmod m(x) = (X_1 \bmod m(x), Y_1 \bmod m(x))$;

$P_2 \bmod m(x) = (X_2 \bmod m(x), Y_2 \bmod m(x))$

It is enough to show that $X_1 \bmod m(x) \neq X_2 \bmod m(x)$ which follows from the Lemma 3.4.

Case(ii): Suppose $X_1 \equiv X_2 \bmod m(x)$.

Suppose $P_1 = P_2$. Then $P_1 \bmod m(x) + P_2 \bmod m(x) = 2P_1 \bmod m(x)$.

Claim:

Denominator $2Y_1$ is not divisible by $m(x)$.

Suppose $2Y_1$ is divisible by $m(x)$. Then, because denominator of X_3 is not divisible by $m(x)$ it would follow from (3.10) that the numerator $(3X_1^2 + A)$ must be divisible by $m(x)$.

This implies that $(3X_1^2 + A) \equiv 0 \bmod m(x).$

(i.e) X_1 is a root modulo $m(x)$ of both the cubic $(X^3 + AX + B)$ and its derivative, contradicting out assumption that there are no multiple roots modulo $m(x)$ for the cubic $(X^3 + AX + B)$.

Hence $2Y_1$ is not divisible by $m(x)$.

(i.e) $Y_1 \bmod m(x) \neq -Y_1 \bmod m(x)$.

Suppose $P_1 \neq P_2$. Since $X_2 \equiv X_1 \bmod m(x)$ and $X_2 \neq X_1$, we can write

$(X_2 - X_1) = (m(x))^r s(x)$, where $r \geq 1$ is chosen such that neither the numerator nor the denominator of $s(x)$ is divisible by $m(x)$.

Since we have assumed that the denominator of $P_1 + P_2$ is relatively prime to $m(x)$, we can use (3.9) to conclude that $(Y_2 - Y_1)$ is of the form,

$$(Y_2 - Y_1) = (m(x))^r t(x) \text{where} t(x) \in T(x). \qquad (3.11)$$

$$\text{Also} Y_2^2 = X_2^3 + AX_2 + B =$$

$$(X_1 + m(x)^r s(x))^3 + A(X_1 + m(x)^r s(x)) + B$$

$$\equiv \left((X_1^3 + AX_1 + B) + m(x)^r s(x)(3X_1^2 + A)\right) \bmod m(x)^{r+1}$$

$$\text{(i.e)}\, Y_2^2 \equiv \left(Y_1^2 + m(x)^r s(x)(3X_1^2 + A)\right) \bmod m(x)^{r+1} \quad (3.12)$$

But since $X_2 \equiv X_1 \bmod m(x)$ and $Y_2 \equiv Y_1 \bmod m(x)$, it follows that $X_1 \bmod m(x) \equiv X_2 \bmod m(x)$ and $Y_1 \bmod m(x) \equiv Y_2 \bmod m(x)$

(i.e) $P_1 \bmod m(x) = P_2 \bmod m(x)$

$$\therefore P_1 \bmod m(x) + P_2 \bmod m(x)$$

$$= 2P_1 \bmod m(x) = O \bmod m(x)$$

iff $Y_1 \equiv Y_2 \equiv O \bmod m(x).$ In this case the numerator of $Y_2^2 - Y_1^2 = (Y_2 - Y_1)(Y_2 + Y_1)$ would be divisible by $m(x)^{r+1}$ and (3.12) would imply that $(3X_1^2 + A) \equiv O \bmod m(x)$ and so X_1 would be a common root of the polynomial $(X^3 + AX + B)$ and its derivative. This is impossible because the cubic polynomial modulo $m(x)$ has no multiple roots.

$\therefore P_1 \bmod m(x) + P_2 \bmod m(x) \neq O \bmod m(x)$

Conversely, Suppose that for all irreducible factors $m(x)$ of $f(x)$, we have $P_1 \bmod m(x) + P_2 \bmod m(x) \neq O \bmod m(x)$ we must show that $(P_1 + P_2)$ has co-ordinates with denominators prime to $f(x)$. Fix some irreducible polynomial $m(x)$ dividing $f(x)$. If $X_2 \not\equiv X_1 \bmod m(x)$ then (3.9) shows that there are no denominators divisble by $m(x)$

If $X_2 \equiv X_1 \bmod m(x)$,

then $Y_1^2 \equiv Y_2^2 \bmod m(x)$ .But,since

$\Rightarrow Y_2 \equiv \pm Y_1 \bmod m(x)$

$P_1 \bmod m(x) + P_2 \bmod m(x) \neq O \bmod m(x)$, we must have $Y_1 \equiv Y_2 \not\equiv 0 \bmod m(x)$

Suppose $P_1 = P_2$, then (3.10) together with the fact that $Y_1 \not\equiv 0 \bmod m(x)$ shows that the co-ordinates of $P_1 + P_2 = 2P_1$ has denominators prime to $m(x)$

Suppose $P_2 \neq P_1$, co-ordinates of $P_1 + P_2$ is as in (3.9). As in the first part write $X_2 = X_1 + (m(x))^r s(x)$ where $s(x) \in T(x)$,is such that neither the numerator nor the denominator of $s(x)$ is divisible by $m(x)$. Using (3.12), we can write $\dfrac{(Y_2^2 - Y_1^2)}{(X_2 - X_1)} = (3X_1^2 + A) \bmod m(x).$ Since $m(x)$ does not divide $Y_2 + Y_1 \equiv 2Y_1 \bmod m(x)$, it follows that there is no $m(x)$ in the denominator of $\dfrac{(Y_2^2 - Y_1^2)}{(X_2 - X_1)(Y_2 + Y_1)} = \dfrac{(Y_2 - Y_1)}{(X_2 - X_1)}$, and hence, by (3.9) $m(x)$ does not divide the denominator of the co-ordinates of $P_1 + P_2$. Hence the theorem.

4. The Factoring Algorithm

This algorithm is an analog of the algorithm of H.W.Lenstra, Jr [11] to factor integers over elliptic curves.

To factor a polynomial $f(x) \in F_p[x]$ one selects an elliptic curve E over the finite ring $R = \dfrac{F_p[x]}{(f(x))}$ and a point P on E.

The following steps are similar to those of Lenstra's algorithm, as presented by Koblitz[17]. All computations are performed modulo p and modulo $f(x)$.

1. The curve E and the point P are generated in some random way, for example by choosing three polynomials A, X, Y in $F_p[x]$ and then setting $B = Y^2 - X^3 - AX$. To ensure that the cubic polynomial $(X^3 + AX + B)$ has no multiple roots modulo $f(x), A, B$ must be chosen such that $4A^3 + 27B^2 \not\equiv 0(\bmod f(x))$

2. The choice of $A, B \in F_p[x]$ must be such that $gcd(4A^3 + 27B^2, f(x)) = 1$. This ensures that the cubic

$(X^3 + AX + B)$ has no multiple roots modulo $m(x)$ for any irreducible divisor $m(x)$ of $f(x)$. If $gcd > 1$ then either $f(x) | (4A^3 + 27B^2)$ (in which case one must make another choice of A and B) or else a non-trivial factor of $f(x)$ has been obtained.

3. Once a pair (E, P) has been chosen, one selects a positive integer k. If the polynomial $f(x) \in F_p[x]$ is $B-$smooth, (if it factors as a product of irreducible polynomials in $F_p[x]$ of norm $\leq B$), then the integer k can be chosen to be $B-$ smooth (all its prime factors are $\leq B$). Suppose k is divisible by powers of small primes $(\leq B)$ which are less than some bound C.

4. Set $k = \prod_{d \leq B} d^{\alpha_d}$ where $\alpha_d = [\log c / \log d]$ is the largest exponent such that $d^{\alpha_d} \leq c$. One tries to compute kP (computations done modulo p and modulo $f(x)$). This computation is uneventful unless one runs into the following difficulty: when attempting to find the inverse of $(X_2 - X_1)$ in formula(3.9) or the inverse of $2Y_1$ in (3.10). One encounters a polynomial that is not prime to $f(x)$. According to proposition (3.4) this will happen when one has some multiple k_1P (a partial sum encountered in the computation of kP) which for some $m(x) | f(x)$ has the property $k_1(P \bmod m(x)) = O \bmod m(x)$. (i.e) the point $P \bmod m(x)$ in the group $E \bmod m(x)$ has order dividing k_1.

5. In the process of using the Euclidean Algorithm to find the inverse modulo $f(x)$ of a denominator which is divisible by $m(x)$, we find the gcd of $f(x)$ with that denominator. That gcd will be a proper divisor of $f(x)$ (unless it is $f(x)$ itself, which would imply, by proposition (3.4), that $k_1(P \bmod m(x)) = O \bmod m(x)$ for all irreducible factors $m(x)$ of $f(x)$ which is highly unlikely). Thus it is seen that as soon as one tries to compute k_1P modulo $f(x)$ for a k_1 which is a multiple of the order of $P \bmod m(x)$ for some $m(x) | f(x)$, one obtains a proper divisor of $f(x)$.

By applying the method again to the factors of $f(x)$ and repeating the process, one eventually gets the canonical factorization of $f(x)$.

If the elliptic curve E happens to be a bad choice (i.e) for each $m(x) | f(x)$, the group $E \bmod m(x)$ has order divisible by a large prime (and so $kP \bmod m(x)$ is not likely to equal $O \bmod m(x)$ for $k \prod_{d \leq B} d^{\alpha_d}$, one has to generate a new pair (E, P) and repeat the process.)

Example: To factor the polynomial $f(x) = x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7$ over F_{23}.

Solution: Let calculations be performed modulo 23 and modulo $f(x)$.

Choose polynomials $A = (4x - 15), X = 14, Y = 1$ in $F_{23}[x]$, $B = (Y^2 - X^3 - AX) = (20 + 13x)$,

$4A^3 + 27B^2 = 3x^3 + 4x^2 + 14 \neq 0$, $gcd(4A^3 + 27B^2, (f(x))) = 1$.

Consider the elliptic curve $E : Y^2 = X^3 + AX + B$ with parameter A, B specified above.

Let $P = (14,1)$ be a point on E. The co-ordinates of $2P$ are calculated using formula (3.10) slope $\lambda = (22 + 2x)$,

$2P = (4x^2 + 19x + 19, 15x^3 + 12x^2 + 9x + 4)$

To find $3P$: Let $P = (X_1, Y_1)$, $2P = (X_2, Y_2)$. Slope $\lambda = \dfrac{Y_2 - Y_1}{X_2 - X_1}$, $gcd(X_2 - X_1, f(x)) = x^2 + 22x + 7$ which is a factor of $f(x)$.

To find the other factors of $f(x)$: Divide $f(x)$ by $x^2 + 22x + 7$ to obtain the quotient $g(x) = x^4 + 21x^3 + 19x^2 + x + 1$.

Let us choose another elliptic curve $E : Y^2 = (X^3 + AX + B)$ and a point $P = (X, Y)$ on it as follows:

$A = (21x^2 + 20x + 21), X = (20x - 4), Y = 1$,

$B = Y^2 - X^3 - AX = 21x^3 + 22x^2 + 11x + 11$, $4A^3 + 27B^2 \neq 0$ and $gcd(4A^3 + 27B^2, f(x)) = 1$. Consider the point $P = ((20x - 4), 1)$

$2P$ is calculated as $2P = (2x^3 + 4x^2 + 5x + 7, 14x^3 + 5x^2 + 10x + 7)$

To find 3P: Let $P = (X_1, Y_1)$, $2P = (X_2, Y_2)$, $gcd(X_2 - X_1, g(x)) = (x^3 + 2x^2 + 4x + 17)$ which is a factor of $g(x)$.

Hence

$$\begin{aligned} & x^6 - 3x^5 + 5x^4 - 9x^3 - 5x^2 + 6x + 7 \\ & = (x^2 + 22x + 7)(x^3 + 2x^2 + 4x + 17)(x - 4) \end{aligned}.$$

5. Conclusion:

The advantage of the elliptic curve method to factor a polynomial $f(x) \in F_p[x]$ is that there are a large number of different curves $E \bmod m(x)$ over $\dfrac{F_p[x]}{(m(x))}$, where $m(x)$ is an irreducible factor of $f(x)$. So trials can be performed with different values of the order $\# E \bmod m(x) = N_m$. The method successfully factors $f(x)$ when the value of N_m is a $B-$smooth number dividing k and there is an irreducible factor $a(x)$ of $f(x)$ such that the order of P in $E \bmod a(x)$ does not divide k.

References

[1] Rudolf Lidl and Harald Niederreiter, "Introduction to Finite fields and their applications," Cambridge University Press, 1986, pp 299.

[2] B.Chor and R.Rivest, "A knapsack-type public key cryptosystem based on arithmetic in finite fields," Advances in Cryptology-Crypto'84, Springer-Verlag 1985, 54-65; revised version in IEEE Transactions on Information Theory IT-34 ,1988, 901-909.

[3] A.M Odlyzko, "Discrete logarithms in finite fields and their cryptographic significance," Advances in cryptology- Eurocrypt 1984, Lecture Notes in Comput. Sci. vol.209, Springer-verlag, Berlin 1985, 224-314.

[4] E.R.Berlekamp, "Factoring polynomials over Large Finite fields," Mathematics of computation, volume 24, Number 111, July 1970, 713-733.

[5] Cantor, D.G and Zassenhaus H, "A new Algorithm for factoring polynomials over finite fields," Mathematics of Computation, 36, 1981, 587-592 .

[6] Berlekamp, E.R, "Algebraic Coding Theory," Mc-Graw Hill, New York, 1968.

[7] Knuth, D.E, "The Art of Computer Programming," vol.2, Seminumerical Algorithms, 2nd edition, Addison-Wesley, Reading, Mass., 1981.

[8] McEliece, "R.J, Factorization of polynomials over finite fields,"

Math.comp.23, 1969, 861-867.

[9] Rabin, M.O, “Probabilistic Algorithms in finite fields,” SIAM J. Computing, 9, 1980, 273-280.

[10] Zassenhaus, H, “On Hensel factorization I,” J.Number Theory 1, 1969, 291-311.

[11] H.W.Lenstra, Jr. “Factoring Integers with Elliptic Curves”, The Annals of Mathematics, Second series, Volume 126, Issue 3 (Nov. 1987), 649-673.

[12] Lawrence C. Washington, “Elliptic Curves, Number Theory and Cryptography,” Second Edition, 2008, Taylor & Francis group, pp 65-71.

[13] H.W.Lenstra, Jr. ‘Elliptic Curves and Number Theoretic Algorithms,” Proceedings of the International Congress of Mathematicians, vol.1,2 (Berkley, Califn, 1986), pp 99-120.

[14] J.H. Silverman, “The Arithmetic of Elliptic curves, Graduate Texts in Mathematics, vol.106, Springer-verlag, New York, 1986.

[15] Lawrence C. Washington, “Elliptic Curves, Number Theory and Cryptography,” Second Edition, 2008, Taylor & Francis group, pp 70.

[16] Neal Koblitz “A Course in Number Theory and Cryptography,” Second edition, Springer, 1994, pp 193-195.