SOFTWARE-HARDWARE SYSTEMS

PSEUDOIRREDUCIBLE POLYNOMIALS:
PROBABILISTIC IRREDUCIBILITY TESTING

L. V. Kovalchuk

Polynomial analogs of pseudoprime numbers are created (Fermat pseudoprimes, Euler pseudoprimes, and strong pseudoprimes). Some of their properties and interrelations are described. Efficient probabilistic algorithms of irreducibility testing are given that are analogs of the Fermat, Solovay–Strassen, and Miller–Rabin algorithms.

Keywords: pseudoprime number, irreducible polynomial, probabilistic algorithm, elliptic curve.

1. STATEMENT OF THE PROBLEM

Irreducible polynomials of large degree (up to 500) are used in various applied problems, for example, see [1, 2]. Sometimes, in particular, in constructing an elliptic curve with definite properties over a field $F_{p^n}$, it is necessary that the degree $n$ of a polynomial be a prime number. It is this requirement on the degree of extension of a field (and, consequently, on the degree of a polynomial) that is required to exclude subexponential algorithms of solution of the discrete log problem (DLP) in a group of points of an elliptic curve [3].

For testing the irreducibility of polynomials, a deterministic algorithm is used that consists of $\binom{n}{2}$ steps [1]. The Euclidian algorithm is executed at every step for determination of the greatest common divisor of polynomials whose degree is no smaller than $n$. This algorithm performs about $\frac{n^2}{2}$ divisions with remainder, which are time-consuming when $n$ is large.

In this article, the author propose probabilistic algorithms for testing the irreducibility of polynomials and show that, in many cases, they turn out to be much more efficient than the deterministic algorithm even during multiple reiteration. The proposed testing algorithm for the case where the degree of a polynomial is a prime number is most efficient. These algorithms are, in a sense, analogs of probabilistic algorithms of testing the primality of a number, but a complete analogy is absent.

2. PSEUDOIRREDUCIBLE FERMAT POLYNOMIALS, CARMICHAEL POLYNOMIALS, AND THE POSSIBILITY OF USING THE FERMAT TEST

We assume that $p$ is a prime number, $f(x), g(x) \in F_q[x]$, $q = p^k$, deg $f = n$, deg $g = m$, and $m < n$.

Definition 1. A polynomial $f(x)$ is called a Fermat polynomial pseudoirreducible to a base $g(x)$ if the following conditions are fulfilled:

1. $f(x)$ is reducible;
2. $(g, f) = 1$;
3. $g(x)^{n-1} \equiv 1$ (mod $f(x)$).
Definition 2. A polynomial $f(x)$ is called a Carmichael polynomial if it is a Fermat polynomial pseudoirreducible to all bases $g(x) \in F_q[x]$ such that we have $(g, f) = 1$.

Examples of Carmichael polynomials are as follows:

\[ f(x) = x(x^2 + x + 1)(x^3 + x^2 + 1) \in F_2[x]; \quad f(x) = (x - 1)(x - 2) \in F_5[x]. \]

THEOREM 1 (on properties of Carmichael polynomials). 1. Let $f(x)$ be a Carmichael polynomial. Then $f(x)$ does not contain squared terms.

2. We assume that $f(x) = g_1(x) \cdots g_k(x)$, $\deg f(x) = n$, $\deg g_i(x) = d_i$, $g_i(x) \neq g_j(x)$, $i \neq j$, and $n = d_1 + \cdots + d_k$ and that $g_i$ are irreducible polynomials. Then $f(x)$ is a Carmichael polynomial $\iff \forall i = 1, k : d_i / n$.

3. For any prime $p$ and integer $s$, there exists an infinite number of Carmichael polynomials over $F_q[x]$, where $q = p^s$.

Proof. 1. We assume that $\exists h(x) : \deg h(x) = m < n, h(x)^2 / f(x)$, and $h(x)$ is an irreducible polynomial. Since $f(x)$ is a Carmichael polynomial, $\forall g(x) \in F_q[x] ((g, f) = 1)$, we have

\[ g(x)^{q^n - 1} = 1 \pmod{f(x)} \Rightarrow f(x) / g(x)^{q^n - 1} - 1 \Rightarrow h(x)^2 / g(x)^{q^n - 1} - 1 \Rightarrow g(x)^{q^n - 1} = 1 \pmod{h(x)^2}. \]

Hence, the order of $g(x)$ as an element of the multiplicative group of the ring $F_q[x]/h(x)^2$ divides the number $q^n - 1$.

We will show that, in the multiplicative group (of order $q^n (q^m - 1)$) of the ring $F_q[x]/h(x)^2$, there are elements whose orders do not divide $q^n - 1$. To this end, in this group, it suffices to specify at least one element whose order is divided by $q$. Such an element is constructed as follows. Let $r(x)$ be the generator of the multiplicative group of the field $F_q[x]/h(x)$. The following two variants are possible: if $r(x)^{q^n - 1} \neq 1 \pmod{h(x)^2}$, then $q$ divides ord $r(x)$ in the multiplicative group of the ring $F_q[x]/h(x)^2$. If $r(x)^{q^n - 1} = 1 \pmod{h(x)^2}$, then we put $r(x) = r(x)1 + h(x)$. As a result, we have

\[ r_1(x)^{q^n - 1} = r(x)^{q^n - 1}(1 + h(x))^{q^n - 1} = (1 + h(x))^{q^n - 1} \pmod{h(x)^2} = 1 + (q^n - 1)h(x) + u(x), \]

where $u(x)$ contains only powers of $h(x)$ beginning with the second one. Therefore, we have $r_1(x)^{q^n - 1} = 1 - h(x)(\text{mod } h(x)^2) \neq 1 \text{ mod } h(x)^2$. Consequently, ord $r_1(x)$ does not divide $q^n - 1$ but ord $r_1(x)$ divides $q^m (q^m - 1)$ and, hence, $q / \text{ord } r_1(x)$.

2. Let $f(x)$ be a Carmichael polynomial. Then we have

\[ \forall b(x) \in F_q[x] ((b(x), f(x)) = 1): b(x)^{q^n - 1} = 1 \pmod{f(x)} \Rightarrow b(x)^{q^n - 1} = 1 \pmod{g_i(x)} \Rightarrow q^{d_i - 1} / q^n - 1. \]

The latter statement follows from the fact that the multiplicative group of the field $F_q[x]/g_i(x)$ is cyclic and, hence, it contains an element of order $q^{d_i - 1}$.

Next, we will use the following simple auxiliary statement: $d_i / n \Leftrightarrow q^{d_i - 1} / q^n - 1$. To prove this statement, it suffices to note that if $d_i$ does not divide $n$, then we have

\[ n = kd_i + r, \quad r < d_i \Rightarrow q^n - 1 = (q^{d_i})^k q^r \neq q^n - 1 = q^r ((q^{d_i})^k - 1) + q^r - 1 \]

and the latter expression is divided by $q^{d_i - 1}$ if and only if $q^{d_i - 1} / q^r - 1$, contrary to the condition $r < d_i$.

Now let $\forall i = 1, k : d_i / n$. Then we have

\[ \forall b(x) ((b(x), f(x)) = 1): b(x)^{q^n - 1} = (b(x)^{q^{d_i} - 1})^k = 1 \pmod{g_i(x)}. \]