sciendo

*Journal of* ELECTRICAL ENGINEERING, VOL 69 (2018), NO5, 400–402

COMMUNICATIONS

# Computing multiplicative inverses in finite fields by long division

**Otokar Grošek, Tomáš Fabšič** *

We study a method of computing multiplicative inverses in finite fields using long division. In the case of fields of a prime order $p$, we construct one fixed integer $d(p)$ with the property that for any nonzero field element $a$, we can compute its inverse by dividing $d(p)$ by $a$ and by reducing the result modulo $p$. We show how to construct the smallest $d(p)$ with this property. We demonstrate that a similar approach works in finite fields of a non-prime order, as well. However, we demonstrate that the studied method (in both cases) has worse asymptotic complexity than the extended Euclidean algorithm.

K e y w o r d s: finite fields, multiplicative inverses

## 1 Introduction

Computing a multiplicative inverse in a finite field is a common operation used in cryptography. For instance, it is a key operation in the cryptographic standard AES [1].

After M. Repka studied the McEliece cryptosystem in [2], he set the question (in personal communication, 2017) if would be possible to find multiplicative inverses in $\mathbb{F}_2[x]/(f(x))$ by dividing one fixed polynomial by field elements. Here we present this problem in a more complex form. The result is positive, but probably not valuable for a real application since the extended Euclidean algorithm (EEA) is asymptotically faster.

A number of methods for calculating a multiplicative inverse for an element $a$ of a finite field are known. Below, we list the methods mentioned in [3]:

1. Multiplying $a$ by elements in the field until the product is one.
2. Calculating the inverse of $a \in \mathrm{GF}(p^m)$ as $a^{-1} = a^{p^m-2}$.
3. By using the extended Euclidean algorithm.
4. By making a logarithm table of the finite field, and performing subtraction in the table.

Another method, which is not mentioned on the webpage [3], is based on so called Wilson's Theorem:

THEOREM 1. *For any* $n$,

$$(n-1)! = -1 \bmod n\,,$$

*if and only if* $n$ *is a prime number.*

From Wilson's Theorem it follows that if $p$ is prime, then for any $a \in \mathbb{Z}_p^*$, we can compute $a^{-1}$ as

$$a^{-1} = \frac{(p-1)\big((p-1)!\big)}{a} \bmod p\,. \tag{1}$$

Thus to find an inverse $\bmod p$ requires one long division and one reduction $\bmod p$.

This approach, although very laborious, has an interesting history [4–6]. J. Waring in Meditationes algebraicae, Cambridge, 1770, p. 218, first published the theorem that $p|1+(p-1)!$ ascribing it to Sir John Wilson (1714–93). J. L. Lagrange was the first to publish a proof also with the converse in Nouv. Mém. Acad. Roy, Berlin, 2, 1773, anne 1771, p. 125.

Also Ibn al-Haytham (c. 1000 AD) solved problems involving congruences using Wilson's theorem [5].

Finally, J. P. M. Binet in Comptes Rendus Paris, 13, 1841, pp. 210–13, employed Wilson's theorem to find the inverse element to $a$ by $-(p-1)!/a$.

This method for finding inverses $\bmod p$ relies on two facts:

Let $d = (p-1)\big((p-1)!\big)$, then

1. for any $a \in \mathbb{Z}_p^*$, $d$ is divisible by $a$, and
2. $d = 1 \bmod p$.

Now a question arises: For a prime $p$, find the smallest possible number $d = d(p)$ satisfying these two conditions. Clearly, $d(p) \le (p-1)\big((p-1)!\big)$, *eg* $d(5) \le 96$, $d(7) \le 4320$. Then for any $a \in \mathbb{Z}_p^*$,

$$d(p)/a \bmod p = a^{-1}. \tag{2}$$

## 2 Finding $d(p)$

It is not difficult to observe that $d(p)$ can be found in two steps. First, find $\ell(p) = \mathrm{LCM}(1, \ldots, p-1)$, and then $h(p) \in \mathbb{Z}_p^*$ such that $h(p)\ell(p) = 1 \bmod p$. The searched number will be $d(p) = h(p)\ell(p)$.

* Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava, Ilkovičova 3, 812 19 Bratislava, Slovakia, {otokar.grosek, tomas.fabsic}@stuba.sk

DOI: 10.2478/jee-2018–0059, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X 

The magnitude of $d(p)$ can be estimated as follows [7]: Let $\pi(n)$ denotes the number of primes not exceeding $n$. Then for any $n \geq 2$, we have

$$\pi(n) \geq \frac{\ln \ell(n)}{\ln n}, \tag{3}$$

or

$$\lim_{n\to+\infty} \frac{\ln \ell(n)}{n} = 1. \tag{4}$$

Thus from a form of the Prime Number Theorem it follows that actually

$$\mathrm{LCM}(1,\ldots,n) \approx e^{\psi(n)},$$

where $\psi$ is the Chebyshev's function, $\psi(x) = x + o(x)$, as $x \to +\infty$. Thus for a large $p$, $d(p)$ is a very large number.

We will illustrate our approach by an example.

EXAMPLE 1. Let $p = 7, a = 5$. Our goal is to find $5^{-1} \bmod 7$. We compute $\ell(7) = 60$, $h(7) = 2$, $d(7) = 120$, $d(7)/5 = 24$ and $5^{-1} = 24 \bmod 7 = 3$.

Now, we will estimate the complexity of this method. We ignore the complexity of computing $d(p)$, since it has to be done only once, and afterwards the same $d(p)$ can be used for computing all multiplicative inverse in $\mathbb{Z}_p^*$. By [8] the following is valid:

1. Complexity of division $d(p)/a$ is $O\big((\log_2 \frac{d(p)}{a})(\log_2 a)\big)$. Thus the complexity of the method can be estimated as $O\big((\log_2 d(p))(\log_2 p)\big)$.
2. Complexity of the extended Euclidean algorithm is $O\big((\log_2 p)^2\big)$.

Thus EEA is asymptotically faster than our new algorithm.

## 3 A generalization for a field GF($p^m$)

In this section, we will use a similar approach for a finite field $\mathrm{GF}(p^m)$ with $m > 1$. The role of primes in the previous section will be played by irreducible polynomials. Thus we start with three well known facts [9].

DEFINITION 1. The Moebius function $\mu$ is the function on $\mathbb{N}$ defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1\,, \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes}, \\ 0, & \text{if n is divisible by the square of a prime.} \end{cases}$$

THEOREM 2. *Let $q = p^m$, where $p$ is prime and $m \geq 1$. The number $N_q(k)$ of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree $k$ is given by*

$$N_q(k) = \frac{1}{k}\sum_{d|k} \mu\big(k/d\big) q^d = \frac{1}{k}\sum_{d|k} \mu(d) q^{\frac{k}{d}}. \tag{5}$$

THEOREM 3. *Let $q = p^m$, where $p$ is prime and $m \geq 1$. The product $I(q,k;x)$ of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree $k$ is given by*

$$I(q,k;x) = \prod_{d|k} (x^{q^d} - x)^{\mu(\frac{k}{d})} = \prod_{d|k} (x^{q^{k/d}} - x)^{\mu(d)}. \tag{6}$$

Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}_p[x]$ of the degree $m$. Our goal is to find a polynomial $d(x)$ in $\mathbb{Z}_p[x]$ such that

1. for any $a(x) \in \mathbb{Z}_p[x]/(f(x)) \setminus \{0\}$, $d(x)$ is divisible by $a(x)$,
2. $d(x) = 1 \bmod f(x)$, and
3. the polynomial $d(x)$ is of the least degree.

To satisfy the first and the third condition, we are searching for

$$\ell(x) = \mathrm{LCM}\{u(x) \in \mathbb{Z}_p[x]/(f(x)), u(x) \neq 0\}. \tag{7}$$

From Theorem 3, it is not difficult to see that

$$\ell(x) = \prod_{k=1}^{m-1} I(p,k;x)^{\lfloor \frac{m-1}{k} \rfloor}. \tag{8}$$

The degree of this polynomial is

$$t = \deg \ell(x) = \sum_{k=1}^{m-1} N_p(k) k \lfloor \frac{m-1}{k} \rfloor. \tag{9}$$

To satisfy the second condition, let $h(x) \in \mathbb{Z}_p[x]/(f(x))$ be such that $h(x)\ell(x) = 1 \bmod f(x)$. The polynomial $d(x) = h(x)\ell(x)$ then satisfies all required conditions.

THEOREM 4. *Let us consider a finite field $\mathbb{Z}_p[x]/(f(x))$, where $f(x)$ is an irreducible polynomial of the degree $m$ in $\mathbb{Z}_p[x]$. Let us consider the polynomial*

$$d(x) = h(x)\ell(x)\,,$$

*where $\ell(x)$ is defined by* (8) *and $h(x)$ is a polynomial in $\mathbb{Z}_p[x]/(f(x))$ such that $h(x)\ell(x) = 1 \bmod f(x)$. Then $d(x)$ satisfies the following property:*
*For any $a(x) \in \mathbb{Z}_p[x]/(f(x))$, $a(x) \neq 0$, we can compute $a(x)^{-1}$ as*

$$a(x)^{-1} = d(x)/a(x) \bmod f(x)\,.$$

*Moreover, the polynomial $d(x)$ is the monic polynomial with the least degree in $\mathbb{Z}_p[x]$ which satisfies this property. The degree of $d(x)$ is*

$$\deg d(x) = t + \deg h(x) < t + m\,,$$

*where $t$ is given by* (9).

EXAMPLE 2. Let $f(x)$ be the AES polynomial, *ie* $f(x) = x^8 + x^4 + x^3 + x + 1$. Then $t = 254$, $\deg h(x) < 8$, $\deg d(x) < 262$. The calculation in $\mathbb{Z}_2[x]$ is as follows:

1. $I(2,1;x) = x(x+1)$
2. $I(2,2;x) = x^2 + x + 1$
3. $I(2,3;x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
4. $I(2,4;x) = x^{12} + x^9 + x^6 + x^3 + 1$
5. $I(2,5;x) = \frac{x^{32}+x}{x^2+x}$
6. $I(2,6;x) = \frac{(x^{64}+x)(x^2+x)}{(x^4+x)(x^8+x)}$
7. $I(2,7;x) = \frac{x^{128}+x}{x^2+x}$

$$\ell(x) = I(2,1;x)^7 I(2,2;x)^3 I(2,3;x)^2 I(2,4;x) I(2,5;x) \\ I(2,6;x) I(2,7;x),$$

$h(x) = x^6 + x^4 + x$, $d(x) = h(x)\ell(x) = (x^6 + x^4 + x)\ell(x)$. The degree and the Hamming weight of $d(x)$ is $\deg d(x) = 260$, $w_H(d(x)) = 88$.

Now, we will compare the complexity of our method with the complexity of the extended Euclidean algorithm. We ignore the complexity of computing $d(x)$, since it has to be done only once, and afterwards the same $d(x)$ can be used for computing all multiplicative inverses in $\mathrm{GF}(p^m)$. We express the complexities in the number of $\mathbb{Z}_p$ operations.

The complexity of the extended Euclidean algorithm for elements in $\mathrm{GF}(p^m)$ is $O(m^2)$ [8].

Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}_p[x]$ of the degree $m$. Let $a(x) \in \mathbb{Z}_p[x]/(f(x)) \setminus \{0\}$. The complexity of the division of $d(x)$ by $a(x)$ is $O\big(\deg a(x)(\deg d(x) - \deg a(x))\big)$. Thus the complexity of our method is $O\big(m(\deg d(x))\big)$.

The value of $\deg d(x)$ is at least $t$, where $t$ is given by (9). By the estimate from page 93 in [9], we have that $N_p(k) \geq 1$ for all $k$. Thus we obtain

$$t \geq \sum_{k=1}^{m-1} k\left\lfloor \tfrac{m-1}{k} \right\rfloor \geq \sum_{k=1}^{m-1} k\big(\tfrac{m-1}{k} - 1\big) = (m-1)\big(\tfrac{m}{2} - 1\big).$$

Therefore EEA is asymptotically faster than our new algorithm.

## 4 Conclusions

We studied the method of finding multiplicative inverses in $\mathbb{Z}_p$ by constructing one fixed integer $d(p)$ with the property that for any $a \in \mathbb{Z}_p^*$, we can compute $a^{-1}$ as $a^{-1} = d(p)/a \bmod p$. We demonstrated that a similar approach works in finite fields $\mathrm{GF}(p^m)$ with $m > 1$, as well. However, we showed that the studied method (both in the case of $\mathbb{Z}_p$ and in the case of $\mathrm{GF}(p^m)$) has worse asymptotic complexity than the extended Euclidean algorithm. For the field $\mathrm{GF}(2^8)$ (which is used in AES, for example), we experimentally found (the experiment was performed in the mathematics software system SageMath) that the presented algorithm is on average approximately 4.4 times slower than the extended Euclidean algorithm.

*Acknowledgment*

This research was sponsored in part by grant VEGA 1/0159/17 and by the NATO Science for Peace and Security Programme under grant G5448.

## REFERENCES

[1] J. Daemen and V. Rijmen, *The design of Rijndael*, Springer-Verlag Berlin Heidelberg, 2002.

[2] M. Repka, "McEliece PKC Calculator", *Journal of Electrical Engineering*, 2014, vol. 65, no. 6, pp. 342–348.

[3] Wikimedia Foundation, Inc.: "Finite Field Arithmetic", Wikipedia: The free encyclopedia, https://en.wikipedia.org/wiki/Finite_field_arithmetic, accessed March 2018.

[4] L. E. Dickson, "History of the Theory of Numbers, Vol. I.", G. E. Stechert & Co., New York, 1934.

[5] J. J. O'Connor and E. F. Robertson, "Abu Ali al-Hasan ibn al-Haytham, MacTutor History of Mathematics archive", http://www-history.mcs.st-and.ac.uk/Biographies/Al-Haytham.html, accessed March 2018.

[6] L. E. Dickson, "History of the Theory of Numbers, Vol. II." G. E. Stechert & Co., New York, 1934.

[7] G. Tenenbaum, "Introduction to Analytic and Probabilistic Number Theory", American Mathematical Society, 2015, third edition.

[8] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1996.

[9] R. Lidl and H. Niederreiter, "Finite Fields", Cambridge University Press, Cambridge, 1984.

Received 16 October 2017

**Otokar Grošek** (Prof, RNDr, PhD) was born in 1950. He graduated at the Comenius University (1973), and was assigned to Professor Štefan Schwarz as a graduate student (PhD-1978), (Prof-1998). He is the Chair of the Institute of Informatics and Mathematics at the Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava. Since 1983 he is working in cryptology.

**Tomáš Fabšič** (Mgr, PhD) was born in 1986. He holds a bachelor's degree in mathematics from the University of Warwick and master's degrees in mathematics from the University of Cambridge and the Comenius University. He completed graduate study under the supervision of Professor Otokar Grošek at the Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava (PhD-2017). Currently, he is a postdoc at the Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava. His research interests lie in cryptology.