

A Theorem related to Multiplicative Order

Abstract: This paper presents a theorem, which is an attempt to relate an element in $GF(p)$ and its modular inverse and also tries to relate order of certain elements in $GF(p)$. The theorem is as follows:

Let $S'(A)$ be the set of elements in $GF(p)$ such that $S'(A) = \{x / O(x,p) = A\}$. Here A should be the factor of $(p-1)$ and $A > 2$, where p is prime, then

$$\sum x = \mu(A) + \frac{1}{2} * T(A) * p;$$

where the summation is over all the elements of set $S'(A)$ and

$O(x,p)$: Order of x with respect to p , (by order it is meant to be multiplicative order).

$\mu(A)$: Mobius function of A .

$T(A)$: Euler's-Totient function of A .

Keywords: $GF(p)$, modular inverse, Order, Totient function, Mobius function.

(1) Introduction:

In Elliptical Curve Cryptography, modular inverse is of very much importance since it is used in the division operation. Computing modular inverse consumes large amount of time and area too. So, this paper tries to relate modular inverse to the corresponding field element in $GF(p)$, so that time complexity can be decreased.

In (2), definitions of modular inverse, Galois field, Mobius function etc are given and results on them which are used further to prove the theorem are given.

In (3), some results and observations which are useful to prove the theorem are mentioned and proved. In (4), the main theorem is proved taking various possible cases of A , i.e; multiplicative order and corollaries related to the theorem are mentioned.

(2) Definitions:

You need not know about ring, field and $GF(p)$ in detail, but some knowledge and understanding of Totient function, Mobius function and multiplicative order is required. So, only definitions of ring, field and Galois field are stated here, these definitions are enough to understand the proof of the theorem.

Ring: A ring (with unity) consists of a nonempty set A together with two operations $+$ and $*$ such that the following properties hold:

- (i) $\langle A, + \rangle$ is an additive group.
- (ii) $\langle A, * \rangle$ is a monoid (i.e, associative magma with an identity).
- (iii) These operations satisfy two distributive laws asserting that $a*(b+c) = a*b + a*c$ and $(a+b)*c = a*c + b*c$ for any three elements a, b, c which belong to A .

Field: A commutative ring k is called a field if k' , the set of non-zero elements of k , form a group with respect to ring multiplication. Thus every non-zero element of k has a multiplicative inverse.

Galois field (GF(p)): A field of integers. If p is prime, then the elements are $\{0, 1, 2, \dots, (p-1)\}$

Mobius function: Mobius function of a number is defined as:

$$\mu(A) = \begin{cases} 0; & \text{if } A \text{ is not square free} \\ 1; & \text{if } A = 1 \\ (-1)^{n(A)}; & \text{if } A \text{ is square free, where } n(A): \text{ number of prime factors of } A. \end{cases}$$

Result (1): $\sum \mu(d) = 0$; where $d = \{x/ x \text{ is a divisor of } A\}$ and the summation is over all possible values of d .

Result (2): If $A = x*y$, then
 $\mu(A) = \mu(x) * \mu(y)$; if $\text{GCD}(x,y) = 1$
 $= 0$; otherwise.
 $\mu(A)$ is multiplicative.

Totient function: Totient function is defined as number of relative primes of A less than A .

$$T(A) = A * (1 - 1/p_1) * (1 - 1/p_2) * \dots * (1 - 1/p_{n(A)})$$

Where $p_1, p_2, p_3, \dots, p_{n(A)}$ are prime factors of A .

Result (3): $\sum T(d) = A$ where $d = \{x/ x \text{ is a divisor of } A\}$ and the summation is over all possible values of d .

Result (4): If $A = x*y$ and $\text{GCD}(x,y) = 1$, then $T(A) = T(x)*T(y)$.

Multiplicative Order: In number theory, given an integer “ a ” and a positive integer n with $\text{GCD}(a,n) = 1$, the multiplicative order of a modulo n is the smallest positive integer “ k ” with

$$a^k \text{ mod } n = 1.$$

Result (5): If $O(a,p) = A$, then order of powers of a will be
 $O(a^k,p) = A/\text{GCD}(A,k)$.

Note: a and $(1/a) \text{ mod } p$ has same order with respect to p for every a which belongs to $\text{GF}(p)$.

Result (6): The order of any subgroup of a group (G) divides the order of G .

Modular inverse: Modular inverse of an element ‘ a ’ in $\text{GF}(p)$ is ‘ b ’ if $a*b \text{ mod } p = 1$ and ‘ b ’ belongs to $\text{GF}(p)$.

Note: If b is the modular inverse of a in $GF(p)$, then $(p-b)$ is the modular inverse of $(p-a)$ in $GF(p)$.

(3) Important results and observations:

Result (7): If A is a factor of $(p-1)$, then for any solution of $x^A \bmod p=1$ in $GF(p)$ except for $x=1$,
 $1+x+x^2+\dots+x^{(A-1)}$ is divisible by p .

Proof: $x^A \bmod p=1$
 $\Rightarrow (x^A - 1) \bmod p=0$
 $\Rightarrow (x-1)*(1+x+x^2+\dots+x^{(A-1)}) \bmod p=0$
 But $x \neq 1$, so $(1+x+x^2+\dots+x^{(A-1)}) \bmod p=0$
 So, $1+x+x^2+\dots+x^{(A-1)}$ is divisible by p .

Explanation for A should be factor of (p-1): By Fermat's Little theorem, for any positive integer a which is relatively prime to p , then $a^{(p-1)} \bmod p=1$. All the solutions of $x^A \bmod p=1$; forms a multiplicative group of order A , as this is a subgroup of $GF(p)-\{0\}$ which is group under multiplication (by definition of field), from result (6), A should divide $(p-1)$.

Result (8): If A is even and A is a factor of $(p-1)$, then for any x in $GF(p)$ except $x=1$,
 $1+x+x^2 \bmod p + x^3 \bmod p + \dots + (x^{(A-1)}) \bmod p = (A/2)p$
 (or)
 Sum of all solutions of $x^A \bmod p=1$ in $GF(p)$ when A is even and a factor of $(p-1)$ is $(A/2)*p$

Proof: Consider $x^A \bmod p=1$ ----- (1)
 Given A is even, so $A = 2*k$
 If x is a solution of (1), then $(-x)$ is also solution to this equation since
 $(-x)^{2k} \bmod p = \{(-1)^{2k} * x^{2k}\} \bmod p$
 $= 1 * x^{2k} \bmod p = x^A \bmod p = 1$.
 But $-x$ doesn't belong to $GF(p)$, add p to make this belong to $GF(p)$.
 So, $(p-x)$ is a solution to equation (1).

L.H.S of the result contains $A/2$ $\{x, (p-x)\}$ pairs. So, the summation equals $(A/2)*(x+p-x)$ which is equal to $(A/2)*p$.

Observation (1): If A is odd and A is a factor of $(p-1)$, then sum of all the solutions of $x^A \bmod p=1$ in $GF(p)$ is $((A-1)/2)*p$.

Result (9): No. of solutions of $O(x,p) = A = T(A)$; if A is a factor of $(p-1)$
 0 ; otherwise

Proof:

Case (1): If A is not a divisor of $(p-1)$, then it is obvious that there are no solutions to $x^A \bmod p=1$; which means that there are no solutions to $O(x,p) = A$.

Case (2): If A is a divisor of (p-1),

Consider an element x which satisfies $O(x,p) = A$. Its powers from 0 to A-1 spans all the solutions of $x^A \bmod p = 1$. From result (5),

$$O(x^k,p) = A/\text{GCD}(A,k)$$

We have to find elements such that $O(x^k,p) = A$, which implies that $\text{GCD}(A,k) = 1$.

So, for all those whose power is relatively prime to A, their multiplicative order is A.

$$\begin{aligned} \text{No. of such elements} &= \text{No. of relative primes to A less than A} \\ &= T(A) \end{aligned}$$

Result (10): If $O(x,p) = A$ and A is a factor of (p-1), then

- (i) $O(p-x,p) = 2*A$; if A is odd.
- (ii) $O(p-x,p) = A$; if $A = 4*k$ where k is any natural number
- (iii) $O(p-x,p) = A/2$; if $A = 4*k+2$ where k is any number.

Proof:

Consider the Geometric series of x with 1st term = x and the common ratio = x, but the multiplication is modular multiplication.

$$x, x \bmod p, x^2 \bmod p, \dots$$

$$(-x)^n \bmod p = \{(-1)^n \bmod p x^n \bmod p\} \bmod p$$

We have to find the least power "k" of (-x) for which $(-x)^k \bmod p = 1$.

If the power "a" of (-x) is even, then $(-x)^a \bmod p = x^a \bmod p$.

If the power "a" of (-x) is odd, then $(-x)^a \bmod p = p - (x^a) \bmod p$.

So, we have to search for (-1) in the Geometric series as mentioned above. We need not search for 1, as $O(x,p) = A$, then we encounter 1 when the power is A for the 1st time.

Case (i): $(-1)^2 \bmod p = 1$.

So, $O(x,p) = 2$.

For $(-1) \bmod p$ to be an element of a multiplicative group of order A, then A should be a multiple of 2.

As A is odd, so $(-1) \bmod p$ is not an element of this group. $x^A \bmod p = 1$ which implies that $(-x)^A \bmod p = (-1) \bmod p$. So, $(-x)^{2A} \bmod p = 1$.

This is the least exponent. So, $O(p-x,p) = 2A$.

Case (ii): $A = 4*k$

$$x^{2*k} \bmod p = (-1) \bmod p = (-x)^{2*k} \bmod p \text{ since } 2*k \text{ is even.}$$

$$x^{4*k} \bmod p = 1 \bmod p = (-x)^{4*k} \bmod p. \text{ So, } A = 4*k \text{ is the least exponent.}$$

So, $O(p-x,p) = A$.

Case (iii): $A = 2*(2*k+1)$

$$x^{(2*k+1)} \bmod p = (-1) \bmod p = \{-(-x)^{(2*k+1)}\} \bmod p \text{ since } 2*k+1 \text{ is odd.}$$

$$\text{So, } (-x)^{(2*k+1)} = 1 \bmod p = 1. \text{ So, } O(p-x,p) = 2*k+1 = A/2.$$

Corollary: If $a*b = (-1) \bmod p$, then $O(b,p)$ takes one of the values of the set $\{O(a,p), O(a,p)/2, 2*O(a,p)\}$

Proof:

Given $a \cdot b \pmod p = (-1)$.

So, $(-b) \pmod p$ is the modular inverse of a . We already stated that a and its inverse has same order. So, $O(p-b, p) \pmod p = O(a, p)$. From the above theorem, depending on the order, it takes one of values of the set $\{O(a, p), O(a, p)/2, 2 \cdot O(a, p)\}$

(4) Main Theorem:

Statement:

Let $S'(A)$ be the set of elements in $GF(p)$ such that $S'(A) = \{x / O(x, p) = A\}$. Here A should be the factor of $(p-1)$ and $A > 2$, where p is prime, then

$$\sum x = \mu(A) + \frac{1}{2} \cdot T(A) \cdot p;$$

where the summation is over all the elements of set $S'(A)$

Proof:

Result (10) is one of the main bases for this theorem. We will prove it taking cases as in the result (10).

Case (i): $A = 4 \cdot k$

$O(x, p) = A$, then $O(p-x, p) = A$. (From result (10))

No. of solutions of $O(x, p) = A$ will be $T(A)$. (From result (9))

So, there are $T(A)/2$ $\{x, p-x\}$ pairs. So, $\sum x = \frac{1}{2} \cdot T(A) \cdot p$.

Case (ii): $A = 2 \cdot k + 1$.

Let's consider how to find relative primes to A and less than A . We take the prime factors (p_1, p_2, \dots) of A and remove their multiples till A , then add multiples of $p_1 \cdot p_2, p_1 \cdot p_3$ and so on as we remove them twice and the process goes until $p_1 \cdot p_2 \cdot \dots \cdot p_n$.

Here same procedure is followed, remove solutions of $A/p_1, A/p_2 \dots$ and add solutions of $A/(p_1 \cdot p_2)$ and so on till $A/(p_1 \cdot p_2 \cdot \dots \cdot p_n)$.

Let $S(k)$ be sum of the solutions of $x^k \pmod p = 1$.

$$\sum x = S(A) - S(A/p_1) - S(A/p_2) - \dots + S(A/(p_1 \cdot p_2)) + \dots + (-1)^n \cdot S(A/(p_1 \cdot p_2 \cdot \dots \cdot p_n))$$

Here we take A to be odd, so all its factors are odd.

$$\text{So, } S(k) = ((k-1)/2) \cdot p$$

But consider $S(A/(p_1 \cdot p_2 \cdot \dots \cdot p_n))$, this can take 2 values.

If $A = (p_1 \cdot p_2 \cdot \dots \cdot p_n)$, then $S(A) = 1$, otherwise $((A/(p_1 \cdot p_2 \cdot \dots \cdot p_n) - 1)/2) \cdot p$.

From this, we can say if A is square free, then $S(A) = ((A/(p_1 \cdot p_2 \cdot \dots \cdot p_n) - 1)/2) \cdot p + 1$

If A is not square free, then $S(A) = ((A/(p_1 \cdot p_2 \cdot \dots \cdot p_n) - 1)/2) \cdot p + 0$

This extra term is nothing but the Mobius function.

$$\sum x = ((A-1)/2) \cdot p - ((A/p_1) - 1/2) \cdot p - \dots + (-1)^n \cdot ((A/(p_1 \cdot p_2 \cdot \dots \cdot p_n) - 1)/2) \cdot p + \mu(A)$$

$$\sum x = p/2 \cdot \{(A - (A/p_1 + A/p_2 + \dots) + (A/(p_1 \cdot p_2) + \dots) \dots) - (1 - nC_1 + nC_2 - \dots + (-1)^n nC_n)\} + \mu(A).$$

Sum all the 1s with A/p_i ; No. of 1s = No. of prime factors of $A = n$

Sum all the 1s with $A/(p_i * p_j)$; No. of 1s = No. of ways we can select 2 prime factors out of prime factors set of $A = nC_2$.

Similarly others can be derived.

$$(1-1)^n = (1-nC_1+nC_2-\dots+(-1)^n nC_n) = 0 \text{ (by Binomial Theorem)}$$

$$\begin{aligned} \sum x &= A * p/2 * (1-(1/p_1+1/p_2+\dots+1/p_n)+(1/(p_1 * p_2)+\dots)\dots) + \mu(A) \\ &= A * p/2 * (1-1/p_1) * (1-1/p_2) * \dots * (1-1/p_n) + \mu(A) \\ &= p/2 * T(A) + \mu(A) \text{ (since } T(A) = A * (1-1/p_1) * (1-1/p_2) * \dots * (1-1/p_n) \text{)} \end{aligned}$$

For every odd, it is proved to be true.

Case (iii): $A = 2 * (2^k + 1)$

$O(x, p) = A$, so $O(p-x, p) = A/2$.

For every x which belongs to $S'(A)$, there exists $p-x$ which belongs to $S'(A/2)$ where $A/2$ is odd.

$$T(A) = T(2) * T(A/2) \text{ (because } \text{GCD}(2, A/2) = 1 \text{ and from result (4))}$$

$$T(2) = 1.$$

$$\text{So, } T(A) = T(A/2). \text{ --- (1)}$$

$$\begin{aligned} \sum x \text{ (over } S'(A)) &= T(A/2) * p - \sum x \text{ (over } S'(A/2)) \\ &= T(A) * p - \sum x \text{ (over } S'(A/2)) \text{ (from eq(1))} \end{aligned}$$

It is proved to be true for every odd factor of $(p-1)$. So, we can substitute for $A/2$.

$$\sum x \text{ (over } S'(A)) = T(A) * p - (1/2) * T(A/2) * p - \mu(A/2).$$

We know $T(A) = T(A/2)$ and $\mu(A) = \mu(2) * \mu(A/2) = -\mu(A/2)$ (from result (2))

Substitute these in above equation

$$\begin{aligned} \sum x \text{ (over } S'(A)) &= T(A) * p - 1/2 * T(A) * p - (-\mu(A)) \\ &= 1/2 * T(A) * p + \mu(A). \end{aligned}$$

Hence the theorem is proved.

In this theorem, n : no. of prime factors of A .

Observations:

If $A=2$, then $\sum x = p-1$.

If $A=1$, then $\sum x = 1$ these are directly seen.

Corollaries:

(1) $\{\sum x \text{ (over } S'(A)) - \mu(A)\} \text{ mod } p = 0$. This can be proved directly using what we have used to prove odd case and result (7), but this is the direct result from above theorem, if we take modulo p operation, we get this result.

(2) Let $r(k, A)$ be the k th relative prime of A and A be square free, then $a^{(-1)} \text{ mod } p = [(\sum a^{\{r(k, A)-1\}}) * \mu(A)] \text{ mod } p$. (expression for modular inverse)

This is a derivative from the previous corollary. If we express each term as power of a , then we get this corollary.

$$(3) \sum \mu(i) = 0 \text{ where } i = \{x/ x \text{ is a divisor of } A\}$$

Let $T(1) = 0$, $T(2) = 2$ for a while from the above observations.

Proof: Take all the factors of A and use the above theorem and all those

$$\sum(\sum x) = p/2 * \sum T(A) + \sum \mu(A)$$

$\sum(\sum x)$ is nothing but the sum of all solutions of $x^A \text{ mod } p = 1$.

If A is even, $\sum T(A) = A$. (because 1 and 2 are both factors of A)

If A is odd, $\sum T(A) = (A-1)/2$ (actually $T(1) = 1$, but for our case $T(1) = 0$)

In both the cases, $\sum \mu(A) = 0$.

(4) If $A = 3$, then $a + (1/a) \text{ mod } p = p-1$. If $A = 4$, then $a + (1/a) \text{ mod } p = p$ and finally if $A = 6$, then $a + (1/a) \text{ mod } p = p+1$. These are the cases where a and $(1/a)$ are the only solutions to $O(x,p) = A$ i.e., $T(A) = 2$.

In these 3 cases, an element and its modular inverse are related as mentioned above.

(5) Conclusion:

It is difficult to built algorithms based on this theorem, because finding order itself is a complex process. As previously said, it is just an attempt to relate an element in $GF(p)$ to its modular inverse. They are directly related if $A = 3, 4$ and 6 . From corollary (2) which is special case, you can find inverse, but it has the same complexity as finding inverse using modular exponential algorithm, that too not valid for all cases.

(6) References:

(1) <http://wikipedia.org>

(2) <http://www.wolfram.mathworld.com>

(3) Linear Algebra: An Introduction to Abstract Mathematics by Robert J.Valenza