# The Disquisitiones Arithmeticae

# of Carl Friedrich Gauss and the group $\mathbf{Z}(p)^*$

**Richard W. Beveridge**

**University of Maine**

Although Gauss did not use any of the terminology of modern group theory in his *Disquisitiones Arithmeticae* of 1801, he did establish some of the most important properties of the multiplicative group of the non-zero integers mod $p$, where $p$ is prime. This group is often referred to as $\mathbf{Z}(p)^*$. Gauss shows that $\mathbf{Z}(p)^*$ is cyclic, and how to determine the number of generators for a particular value of $p$. He also defines the order of an element and shows that this order must divide $p-1$. He then proves that for each factor of $p-1$, there exist elements of that order, and that the number of elements of order $t$ is equal to $\phi(t)$, making use of Euler's phi-function. Gauss' ideas regarding $\mathbf{Z}(p)^*$ are outlined mainly in Section III of the *Disquisitiones Arithmeticae*, although his proofs sometimes rely upon material from Section II.

The fact that $\mathbf{Z}(p)^*$ is cyclic is fairly easily explained in that it is the multiplicative group of a finite field. The proof of this theorem, though, at least in [5] and [8], uses many of the same arguments used by Gauss in *Disquisitiones Arithmeticae*. The bulk of the material that follows in this paper is the work of Gauss, although it has been given modern notation and been reordered to make the presentation more clear to the modern reader. Although Gauss did not discuss $\mathbf{Z}(p)^*$ as a quotient group, these ideas appear in rudimentary form in his discussion of residues in Section I . Without explicitly stating as much, Gauss implies the structure of what are today called residue classes by focusing his discussion on the "least positive residues."

**Preliminaries**

In considering $\mathbf{Z}(p)^*$, we will first establish that $\mathbf{Z}(p)^*$ constitutes a group whenever $p$ is a prime number. $\mathbf{Z}(p)^*$ must satisfy the following conditions

i) Closure:

Given any two elements $a, b \in \mathbf{Z}(p)^*$, their product $ab$ either is an element of $\mathbf{Z}(p)^*$ or it is not. If it is not an element of $\mathbf{Z}(p)^*$, then $\exists\ q, r \in \mathbf{Z}$, with $0 \le r < p$ such that $ab=pq+r$.

$\therefore\ ab \equiv r \pmod{p}$.

ii) Associativity: multiplication is associative

iii) Identity: $\forall x \in \mathbf{Z}, x*1=1*x=x$

iv) Inverses: $\forall\ x \in \mathbf{Z}(p)^*,\ \exists\ x^{-1} \in \mathbf{Z}(p)^*$, such that $x * x^{-1} \equiv 1 \pmod{p}$.

***Proof:***

Each element $x \in \mathbf{Z}(p)^*$ has the property $\gcd(x, p) = 1$. Given $x \in \mathbf{Z}(p)^*$, $x < p$, the existence of an inverse implies that $\exists\ \alpha \in \mathbf{Z}(p)^*$ such that $x * \alpha \equiv 1 \pmod{p}$. This implies that $x * \alpha = n*p + 1$ for some $n \in \mathbf{Z}$.

Because $\gcd(x, p) = 1$, there exists a linear combination $xl + pm = 1$, $l,m \in \mathbf{Z}$.

If we choose $\alpha \equiv l \pmod{p}$ and $n = -m$, then each $x \in \mathbf{Z}(p)^*$ will have an inverse.

In fact, in $\mathbf{Z}(n)^*$, where n is not prime, if an element $x$ possesses an inverse, then $\gcd(x,n) = 1$.

***Proof by contradiction:***

Assume that $x \in \mathbf{Z}(n)^*$ possesses an inverse $x^{-1}$, with $x * x^{-1} \equiv 1 \pmod{n}$, but $\gcd(x,n) \neq 1$. If $x * x^{-1} \equiv 1 \pmod{n}$, this implies that $xx^{-1} = nq + 1$, for some $q \in \mathbf{Z}$. If $\gcd(x,n) \neq 1$, then $\gcd(x,n) = k > 1$.

Let $\frac{x}{k} = x_k$ and $\frac{n}{k} = n_k$, with $x_k, n_k \in \mathbf{Z}$.

So, if $xx^{-1} = nq + 1$, then $\frac{xx^{-1}}{k} = \frac{nq}{k} + \frac{1}{k} \quad \Rightarrow x_k x^{-1} = n_k q + \frac{1}{k}$

With $x_k, x^{-1}, n_k, q \in \mathbf{Z}$, then $\frac{1}{k} \in \mathbf{Z}$. However, if $k>1$, then $\frac{1}{k} \notin \mathbf{Z}$.

$\therefore$ If $x \in \mathbf{Z}(n)^*$ has an inverse, then $\gcd(x,n) = 1$.

**Roots of Polynomials**

This last proposition is related to a more powerful result of Gauss from *Disquisitiones Arithmeticae* that is important in proving that $\mathbf{Z}(p)^*$ is cyclic. It implies the converse of the above statement, that if $\gcd(x,n) = 1$, then $x^{-1}$ exists. In Article 24 of *Disquisitiones Arithmeticae*, Gauss shows that any congruence $ax+b \equiv c \pmod{m}$, can be solved for $x$, if $\gcd(a,m) = 1$.

Article 24. *Let a,b be given numbers and x an indeterminate or variable number. The expression ax+b can be made congruent to any number relative to a modulus m, provided m is prime relative to a.*[4]

***Proof***

Essentially Gauss is saying that $ax + b \equiv c \pmod{m}$ is solvable, so long as $(a,m) = 1$. This congruence reduces to $ax \equiv c - b \pmod{m}$, and we may then consider $ax \equiv e \pmod{m}$, where $e$ is the least positive residue of $c - b$. So, we must show that $\forall\, 0 \le e < m,\ \exists\, x,$ $0 \le x < m$ such that $ax \equiv e \pmod{m}$.

If $(a,m) = 1$, then the least positive residues of each multiple of $a$ up to $(m-1)$, $\{0, a, 2a, 3a, \ldots, (m-1)a\}$ will all be distinct. We may show this by contradiction.

If $\exists\, na$ and $ka$, with $0 \le n < m$, and $0 \le k < m$, with the least positive residues of $na$ and $ka$ equal, then $na = q_n m + r$ and

$ka = q_k m + r.$

This then implies that $(n-k)a = (q_n - q_k)m$. Obviously $(q_n - q_k)m$ is an integer multiple of $m$. Therefore, since $(a,m) = 1$, the factors of $m$ must be contained in $(n-k)$ and $(n-k) = m\alpha$, $\alpha \in \mathbf{Z}$. However, $0 \le n < m$, and $0 \le k < m$, then $0 \le |n-k| < m$. If $(n-k) = m\alpha$, with $\alpha \in \mathbf{Z}$, and $0 \le |n-k| < m$, then $\alpha = 0$, which implies that $n = k$.

Therefore, if $(a,m) = 1$, then the least positive residues of each multiple of $a$ up to $(m-1)$, $\{0, a, 2a, 3a, \ldots, (m-1)a\}$ will all be distinct. Since there are $m$ distinct residues, all less than $m$, they must exhaust all possible values between 0 and $m-1$, so, $\forall\, 0 \le e < m,\ \exists\, x,$ $0 \le x < m$ such that $ax \equiv e \pmod{m}$.

Article 24 shows that $ax + b \equiv c \pmod{m}$ is solvable if $(a,m) = 1$. Article 26 goes on to show that, given a particular solution of the congruence $ax + b \equiv c \pmod{m}$, say

$x = v$, then all solutions of the congruence will be congruent to $v$. Because of this, we may say that a linear congruence of this type permits one and only one solution, $x \equiv v \pmod{m}$. For instance, if $x = t$ is also a solution to $ax + b \equiv c \pmod{m}$, then $av + b \equiv at + b \pmod{m}$, which implies that $av \equiv at \pmod{m}$. If $av \equiv at \pmod{m}$, then $m$ must divide $av - at$, so

$$a(v - t) = m\alpha, \ \alpha \in \mathbf{Z}.$$

Here again, if we know that $a$ and $m$ are relatively prime, then the factors of $m$ must appear in $v - t$, so we can say $v - t = m\beta$, which implies that $m$ divides $v - t$, so $v \equiv t \pmod{m}$.

Gauss uses this result for an inductive proof of the fact that polynomials of degree $n$ in mod $p$, where $p$ is prime, have at most $n$ roots. This property of polynomials in mod $p$ is the key to proving that $\mathbf{Z}(p)^*$ is cyclic.

Article 43. *A congruence of the $m^{th}$ degree*

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \text{etc.} + Mx + N \equiv 0$$

*whose modulus is a prime number p which does not divide A, cannot be solved in more than m different ways, that is, it cannot have more than m noncongruent roots relative to p.* [4]

***Proof***

Gauss uses the previous result as the initial step for a proof by induction, so we have shown that this theorem is true when $m = 1$. Next we must assume that it is true for all values up to a particular value of $m$, say $k - 1$, then show that it is also true for $k$.

If we consider the congruence of degree $k$ and assume that there exist $k+1$ roots of this congruence, we may show that this leads to a contradiction.

Given

$$Ax^k + Bx^{k-1} + Cx^{k-2} + \text{etc.} + Mx + N \equiv 0 \pmod{p},$$

and $k+1$ roots ($x \equiv \alpha,\ x \equiv \beta,\ x \equiv \gamma,\ x \equiv \delta,$ etc.), we can make the substitution $x = y + \alpha$. Then the congruence becomes

$$A(y+\alpha)^k + B(y+\alpha)^{k-1} + C(y+\alpha)^{k-2} + \text{ etc. } + M(y+\alpha) + N \equiv 0 \pmod{p}.$$

In Article 41, Gauss proves the result that $\mathbf{C(p, n)} \equiv 0 \pmod{p}$, for a prime number $p$ and $n \neq 0$ and $n \neq p$. So, the above congruence becomes

$$A(y^k + \alpha^k) + B(y^{k-1} + \alpha^{k-1}) + C(y^{k-2} + \alpha^{k-2}) + \text{ etc. } + M(y+\alpha) + N \equiv 0 \pmod{p}$$

which implies that

$$Ay^k + By^{k-1} + \ldots + My + (A\alpha^k + B\alpha^{k-1} + \ldots + M\alpha + N) \equiv 0 \pmod{p}.$$

Because $\alpha$ is a root of the original congruence, $(A\alpha^k + B\alpha^{k-1} + \ldots + M\alpha + N)$ is congruent to zero. Therefore, we state that

$Ay^k + By^{k-1} + \ldots + My \equiv 0 \pmod{p}$, and

$y(Ay^{k-1} + By^{k-2} + \ldots + M) \equiv 0 \pmod{p}$.

Now, $y \equiv 0$ is a root of this congruence, as are $y \equiv \beta - \alpha \pmod{p}$, $y \equiv \gamma - \alpha \pmod{p}$, $y \equiv \delta - \alpha \pmod{p}$, etc.

The reduced congruence contained in parentheses is a congruence of degree $k-1$, which possesses $k$ distinct roots:

$y \equiv \beta - \alpha,\ y \equiv \gamma - \alpha,\ y \equiv \delta - \alpha,$ etc.

This contradicts our assumption that the number of roots of all congruences of degree less than $k$ must be no more than the degree of the congruence. Therefore, if the number of roots of all congruences of degree less than $k$ is no more than the degree of the congruence, then this must also be true for congruences of degree $k$.

## The Order of Elements in $\mathbf{Z}(p)^*$ and Lagrange's Theorem

Gauss uses several important lemmas related to the order of elements in $\mathbf{Z}(p)^*$ in his proof that $\mathbf{Z}(p)^*$ is cyclic. In the first article of Section III of *Disquisitiones Arithmeticae,* he shows that all elements of $\mathbf{Z}(p)^*$ will have finite order. It is presented nearly verbatim as it appears in [4].

Article 45. *In any geometric progression 1, a, aa, $a^3$, etc., outside of the first term 1, there is still another term $a^t$ which is congruent to unity relative to the modulus p when p is prime relative to a; and the exponent t is $< p$.* [4]

***Proof:***

Since $p$ is prime relative to $a$, and therefore any power of $a$, no term in the progression will be congruent to 0 mod $p$, but each will be congruent to one of the numbers from the least residue class $\{1, 2, 3, ..., p-1\}$. Since the number of these is $p$ -1, it is clear that if we consider more than $p-1$ terms of the progression, not all of them can have distinct least residues. So, among the $p$ terms 1, $a$, $aa$, $a^3$,.....,$a^{p-1}$ there must be at least one congruent

pair. Let us say then that $a^m \equiv a^n \pmod{p}$, with $m > n$. Dividing by $a^n$ we get $a^{m-n} \equiv 1 \pmod{p}$ with $0 < m - n < p$.

Article 49 is another important step in proving that $\mathbf{Z}(p)^*$ is cyclic. Here, Gauss produces a result analogous to Lagrange's Theorem on the order of subgroups of a finite group.

Article 49. *If p is a prime number that does not divide a, and if $a^t$ is the lowest power of a that is congruent to unity relative to the modulus p, the exponent t will either equal p-1 or be a factor of this number.* [4]

***Proof:***

Article 45 shows that $t \leq p-1$, so what remains to be shown is that $t$ is a factor of $p-1$. If $t = p-1$, the theorem is satisfied. With $t < p-1$, if we consider the least positive residues of 1, $a$, $aa$, $a^3$,....., $a^{t-1}$, these values must all be distinct. If $\exists\, a^m \equiv a^n \pmod{p}$ (supposing $m > n$), then we would have $a^{m-n} \equiv 1 \pmod{p}$, with $m - n < t$, which would contradict our assumption that $t$ is the lowest power of $a$ that is congruent to unity relative to the modulus $p$. The least positive residues (1, $a$, $aa$, $a^3$,....., $a^{t-1}$) must be contained in the series of numbers 1, 2, 3,....., $p-1$. If we let $A$ designate this set of least positive residues, it is evident that the cardinality of $A$ is $t$.

Now, we may choose a number, $b$, from the collection 1, 2, 3,....., $p-1$, that is not contained in $A$ (if not, then $t = p-1$, and we are done). Consider the least residues of the

products $b, ba, baa, ba^3$, etc., and designate this collection as the set *B*. *B* will also possess $t$ terms. Two important facts are true of the set *B*.

(1) Each of the terms will be distinct.

(2) $A \cap B = \varnothing$.

For (1), let us assume that $ba^m \equiv ba^n \pmod{p}$. This would imply that $a^m \equiv a^n \pmod{p}$, which contradicts the fact that the elements of *A* are all distinct.

If (2) were not true, then $ba^m \equiv a^n \pmod{p}$.

For $m < n$, then $b \equiv a^{n-m} \pmod{p}$, which contradicts our assumption that $b \notin A$.

If $m > n$, then we can multiply both sides by $a^{t-m}$, which would give us

$ba^t \equiv a^{t+n-m} \pmod{p}$, or, since $a^t \equiv 1 \pmod{p}$, $b \equiv a^{n-m} \pmod{p}$.

Here again, this contradicts the assumption $b \notin A$.

If all elements from 1, 2, 3,....., $p-1$ are contained in *A* and *B*, then we are done and

$$\frac{p-1}{2} = t.$$

If there are numbers left, we may choose a number $c$, such that $c \notin A$ and $c \notin B$. Multiply $c$ by each element from *A* and consider the set of least residues *C*. Similar to the process above, there will be *t* elements of *C*, all of which are distinct, and $A \cap C = \varnothing$.

It will also be true that $B \cap C = \varnothing$. Given $ca^m \equiv ba^n \pmod{p}$, then (as above),

if $m < n$,

$c \equiv ba^{n-m} \pmod{p}$

or, if $m > n$

$c \equiv ba^{t+n-m} \pmod{p}$.

If, now, the $3t$ numbers contained in $A \cup B \cup C$ exhaust all possibilities 1, 2, 3,....., $p-1$, then we are done and $\frac{p-1}{3} = t$. If there are still other numbers remaining, we may then continue the process, in each case generating $t$ elements which are distinct from one another, and also distinct from the elements in the previous sets. Because the collection $1,2,3,\ldots,p-1$ is finite, at some point all values will be exhausted. At this point, $\frac{p-1}{n} = t$.

**Proving $\mathbf{Z}(p)^*$ Cyclic**

Articles 52, 53 and 54 essentially prove that $\mathbf{Z}(p)^*$ is a cyclic group. Gauss provides a separate proof that $\mathbf{Z}(p)^*$ is cyclic in Article 55, and states at the end of this article that the demonstration in 52, 53 and 54 is less direct than that of 55. However, Article 55 depends squarely upon the result of 52, 53 and 54 in stating that there must always exist an element whose order is equal to a given divisor of $p-1$. For this reason, I will present only the first proof Gauss provides that $\mathbf{Z}(p)^*$ is cyclic - that contained in articles 52, 53 and 54.

The proof in Articles 52, 53 and 54 itself depends upon Article 39 which states that the sum of Euler's phi function for all the divisors of a number A will equal A.

Article 39 *If $a, a', a'', \text{etc.}$ are all the divisors of A (including unity and A itself), we will have*

$$\phi a + \phi a' + \phi a'' + \text{etc.} = A \text{ [4]}$$

***Proof***

For each divisor of $A$, generate the integer $A/a$ and multiply it by all integers less than $a$ that are relatively prime to $a$. Two important facts will be true.

1) All of the resulting numbers will be unequal.

It is clear that all numbers generated by the same divisor of $A$ will be unequal. If we assume that two different divisors could generate the same number from this process, then $(A/a')\mu = (A/a'')\nu \Rightarrow \mu a'' = \nu a'$. If we suppose that $a' > a''$, with $\mu$ and $a'$ relatively prime, then $a' \mid a''$, but we assumed that $a' > a''$, therefore all of the numbers must be unequal. The same argument may be made for $a'' > a'$

2) All of the numbers from 1 to $A$ will be included in this collection.

If we choose a number $t < A$, and consider the $\gcd(A,t) = \delta$, then $A/\delta$ and $t/\delta$ will be relatively prime. $A/\delta$ will be the divisor from the collection $a, a', a'', etc.$ that will generate the number $t$. When $A/(A/\delta)$ is calculated, the result will, of course, be $\delta$. Because $A/\delta$ and $t/\delta$ are relatively prime, then $t/\delta$ will be one of the numbers by which $\delta$ is multiplied, generating the desired result $t$.

As these two conditions are satisfied, then $\phi a + \phi a' + \phi a'' + \text{etc.} = A$.

Article 52: *Suppose we are given numbers which are to be made congruent to unity by raising to a power. We know that for the exponent involved to be of lowest degree it must be a divisor of* $p-1$. *The question arises whether all divisors of* $p-1$ *enjoy this property. And if we take all numbers [ less than* $p-1$*], how many are there for each exponent?...Thus we must find out how in this respect the numbers 1,*

*2, 3, ... , $p-1$ should be distributed among the individual factors of the number $p-1$. In brief, if $d$ is one of the divisors of the number $p-1$ (among these 1 and $p-1$ itself must be included•), we will designate by $\psi d$ the number of positive numbers less than $p$ whose $d^{th}$ power is the lowest one congruent to unity. To make this easier to understand, we give an example. For p=19... $\psi 1 = 1$, $\psi 2 = 1$, $\psi 3 = 2$, $\psi 6 = 2$, $\psi 9 = 6$, $\psi 18 = 6$. A little attention shows that with each exponent there are associated as many numbers as there are numbers relatively prime to the exponent not greater than it. In other words in this case... $\psi d = \phi d$. Now we will show that this observation is true in general.*[4]

***Proof:***

Consider an element $a \in \mathbf{Z}(p)^*$ of order $d$, where $d$ is a divisor of $p-1$. We know that $a, a^2, a^3, ...., a^d$ are all distinct. Furthermore, $a^d \equiv 1 \pmod{p}$, $(a^2)^d \equiv 1 \pmod{p}$, $(a^3)^d \equiv 1 \pmod{p}$ …etc. This implies, then, that $a, a^2, a^3, ...., a^d$ are all roots of the congruence $x^d \equiv 1 \pmod{p}$. There cannot be more than $d$ roots of this equation, so all elements whose order is $d$ are found in the collection $a, a^2, a^3, ...., a^d$.

If $k < d$ and $(k,d) = 1$, then $a^k$ will be of order *d*. From article 24, we know that if $(k,d) = 1$, then $\exists m$, such that $km \equiv 1 \pmod{d}$. Therefore we can say that $a^{km} \equiv a \pmod{p}$. If there exists $e < d$ such that $(a^k)^e \equiv 1 \pmod{p}$, then $(a^{ke})^m \equiv 1^m \pmod{p}$ or $a^{kme} \equiv 1 \pmod{p}$, which implies that $a^e \equiv 1 \pmod{p}$ with $e < d$, which contradicts our initial assumption that $a$ is of order $d$.

If, on the other hand, $(k, d) \neq 1$, then $a^k$ will not be of order $d$. If we say that $k$ and $d$ share a divisor $\delta$, where $k = n\delta$ and $d = m\delta$, with $n, m \in \mathbf{Z}$. We know that

• In including $p-1$, Gauss implies that $\mathbf{Z}(p)^*$ is cyclic.

$(a^n)^d \equiv 1 \pmod{p}$, $\forall n \in \mathbf{N}$, so $(a^{\frac{k}{\delta}})^d \equiv 1 \pmod{p}$ and $(a^k)^{\frac{d}{\delta}} \equiv 1 \pmod{p}$ with $\frac{d}{\delta} \in \mathbf{Z}$ and $\frac{d}{\delta} < d$. Therefore $a^k$ will be of order less than $d$ if $(k, d) \neq 1$.

This implies that there are as many elements of order $d$ as there are positive numbers less than $d$ and relatively prime to $d$. This conclusion depends on the existence of one element of order $d$, so we could say that either $\psi(d)$ is zero or $\psi(d) = \phi(d)$.

Given $d, d', d''$,....etc. the divisors of $p-1$, we know that

$\psi(d) + \psi(d') + \psi(d'') + ....\text{etc.} = p-1$ and that

$\phi(d) + \phi(d') + \phi(d'') + ....\text{etc.} = p-1$.

If one or more of the terms $\psi(d), \psi(d'), \psi(d'')$,....etc. were equal to zero, then another of them would need to be larger than its corresponding $\phi$ value. However we have just seen that each $\psi$ may be equal to the corresponding $\phi$ or equal to zero but in no way greater than $\phi$.

$\therefore \psi(d) = \phi(d)$ *for all divisors of* $p-1$.

From this we may conclude that since there always exists at least one number less than $p-1$ and relatively prime to $p-1$ there will be at least one element of order $p-1$, i.e. a generator of the group. If we call this element $a$, then $\mathbf{Z}(p)^* = \langle a \rangle$ and $\mathbf{Z}(p)^*$ is cyclic.

The multiplicative group $\mathbf{Z}(p)^*$ is a very interesting mathematical structure from a purely theoretical standpoint. It incorporates many important ideas of abstract algebra and number theory. As has been shown by the work of Whitfield Diffie, Martin Hellman, Ron Rivest, Adi Shamir, Len Adelman, Bruce Schneier, Neal Koblitz and many others, these highly theoretical ideas can also be applied in the field of cryptography. The application of

number theory and the theories of finite groups and fields in computer science has led to some fascinating new ideas and extensions of existing areas of research. It can never be known when or where mathematical theories may be applied. The essential role that the ideas of Euler and Gauss continue to play our society indicates the importance of continued research in pure mathematics.

References


[1] Bühler, W.K., ***Gauss A Biographical Study***, Springer-Verlag, 1981.

[2] Burton, David M., ***Elementary Number Theory***, 3rd ed., Wm. C. Brown Publishers, 1994.

[3] Diffie, Whitfield, Forward to ***Applied Crytography*** by Bruce Schneier, 2nd ed., John Wiley & Sons, 1996.

[4] Gauss, Carl Friedrich, ***Disquisitiones Arithmeticae***, Yale University Press, 1966. (Translation from the 1870 Latin 2nd ed. by Arthur A. Clarke, S.J.)

[5] Hungerford, Thomas W., *Abstract Algebra, An Introduction*, Saunders College Publishing, 1990.

[6] Kleiner, Israel, "The Evolution of Group Theory: A Brief Survey," Mathematics Magazine, vol. 59, n. 4, Oct. 1986.

[7] Koblitz, Neal, ***A Course in Number Theory and Cryptography***, 2nd ed., Springer-Verlag, 1994.

[8] Rotman, Joseph J., ***A First Course in Abstract Algebra***, 2nd ed., Prentice-Hall, 2000.

[9] Wussing, H., ***The Genesis of the Abstract Group Concept***, M.I.T. Press, 1984. (Translation from the 1969 German edition by A. Shenitzer)