

ON THE THEORY OF CUBIC RESIDUES

C. F. Gauss

[1.]

$p = mm + 3nn$ is a prime number.

One sets for any whole number x divisible by

$$\left[\frac{2mx}{p} \right] = \alpha, \left[\frac{(3n-m)x}{p} \right] = \beta, \left[\frac{(-3n-m)x}{p} \right] = \gamma.$$

from this, as is easily seen, the sum of three pure fractions will be,

$$\frac{2mx}{p} - \alpha + \frac{(3n-m)x}{p} - \beta + \frac{(-3n-m)x}{p} - \gamma$$

and therefore must lie between the limits 0 and 3 exclusive; however, since the same sum = $-\alpha - \beta - \gamma$, and thus is a whole number, it can have no other value than +1 and +2. It is thus either

$$\alpha + \beta + \gamma = -1 \text{ or } \alpha + \beta + \gamma = -2.$$

From this follows further, that the limits α, β, γ could not all be congruent to each other with respect to modulus 3; among the differences $\alpha - \beta, \beta - \gamma, \gamma - \alpha$ will thus at least one (and even for this reason at least still one, because the sum of all is = 0) which is not $\equiv 0$. Still less however could the magnitudes α, β, γ be incongruent among each other, because the otherwise, regardless of order, be congruent to the numbers 0, 1, 2 and thus their sums must be divisible by 3; it will follow from the differences $\alpha - \beta, \beta - \gamma, \gamma - \alpha$ [gewiss-certain, sure] one, however, also only to be one, which is $\equiv 0$. There is consequently three cases, which are mutually exclusive

- I. If $\beta \equiv \gamma \pmod{3}$
- II. If $\gamma \equiv \alpha \pmod{3}$
- III. If $\alpha \equiv \beta \pmod{3}$.

which of these three cases it is [statthat], depends on x ; we well therefore divide these three cases all numbers divisible by p into 3 classes according to [Ausgabe-proportion, measure, requirement], in the first namely set that, where

the first; in the second, that where of the second; in the third that where third class occurs.

First Theorem: All numbers congruent with respect to modulus p belong on the same class.

Second Theorem: Similarly, however associated numbers with opposite signs belong to one class. From this is clear, that one merely needs the numbers $1, 2, 3, \dots, \frac{1}{2}(p-1)$ to classify, about immediately could all remainingto classify(?)

Third Theorem: The numbers $(3n-m)x, 2mx$ belong in two successive classes.

Fourth Theorem: Thus if $\frac{2n-m}{3m} \equiv f$, therefore

$$1 + f + ff \equiv 0 \pmod{p}, \quad 1 \equiv f^3 \pmod{p},$$

then x and the residues of fx, ffx belong in three successive classes in reverse order.

Example of the Classification

$$p = 7 = 4 + 3, \quad 4, 1, -5$$

I. 3. 4.
II. 2. 5.
III. 1. 6.

$$p = 13 = 1 + 12, \quad 2, 5, -7$$

I. 3. 6. 7. 10.
II. 4. 5. 8. 9.
III. 1. 2. 11. 12.

$$p = 19 = 16 + 3, \quad 8, -1, -7$$

I. 1. 2. 9. 10. 17. 18.
II. 3. 4. 8. 11. 15. 16.
III. 5. 6. 7. 12. 13. 14.

$$p = 31 = 4 + 27, \quad 4, 7, -11$$

I. 5. 9. 10. 11. 15. 16. 20. 21. 22. 26.
II. 6. 7. 12. 13. 14. 17. 18. 19. 24. 25.
III. 1. 2. 3. 4. 8. 23. 27. 28. 29. 30.

$$p = 37 = 25 + 12, \quad 10, 1, -11$$

I. 7. 8. 9. 10. 17. 18. 19. 20. 27. 28. 29. 30.
II. 4. 5. 6. 11. 15. 16. 21. 22. 26. 31. 32. 33.
III. 1. 2. 3. 12. 13. 14. 23. 24. 25. 34. 35. 36.

$$p = 43 = 16 + 27, \quad 8, 5, -13$$

I.	7.	8.	14.	15.	16.	20.	21.	22.	23.	27.	28.	29.	35.	36.
II.	6.	11.	12.	13.	17.	18.	19.	24.	25.	26.	30.	31.	32.	37.
III.	1.	2.	3.	4.	5.	9.	10.	33.	34.	38.	39.	40.	41.	42.

7, 2 - p	1	-ρρ	ρ	13, 3 - p	1	1 - ρ	-ρρ
	-1	ρρ	-ρ		1 - ρρ	ρ	ρ - ρρ
					-1	-1 + ρ	ρρ
					-1 + ρρ	-ρ	-ρ + ρρ

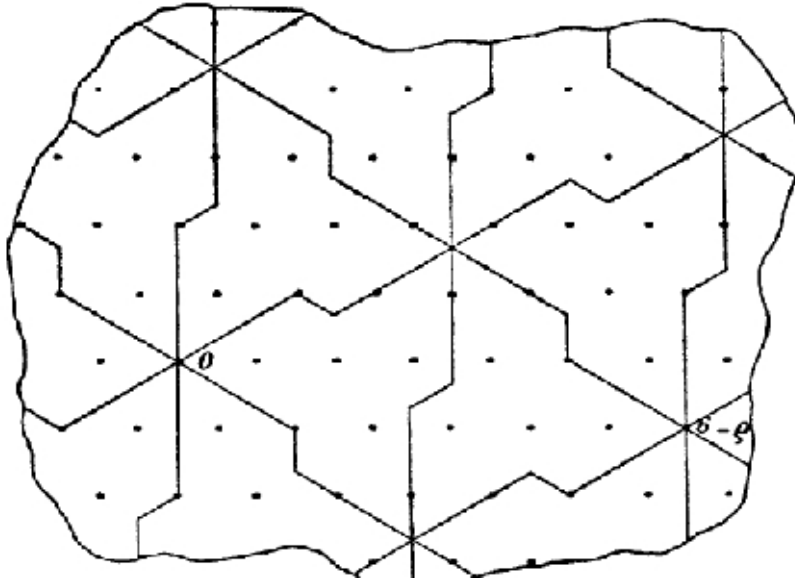


Figure 1: Schema for 34.

[2]

1. Every whole function $\equiv \alpha - \beta x \pmod{1+x+xx}$.
2. $(1 + x + xx)$
3. $P \equiv Q \pmod{1 + x + xx, R}$
4. If $R \equiv R' \pmod{1 + x + xx}$ $1 + x + xx, R \equiv R' \pmod{1 + x + xx, R'}$.

5. If $R' = \alpha + \beta x$, then the least residue of $(P-Q)(\alpha + \beta x x) \pmod{(1+x+xx)}$ must be divisible by $(\alpha\alpha - \alpha\beta - \beta\beta)$.

6. Rule for prime and composite functions.

7. There is in all $\alpha\alpha - \alpha\beta - \beta\beta$ incongruent functions mod. $(1+x+xx, \alpha + \beta x)$, which are congruent to the numbers $1, 2, \dots, \alpha\alpha - \alpha\beta - \beta\beta$.

8. $(1+x+xx)$

9. $\alpha\alpha - \alpha\beta - \beta\beta \equiv \alpha + \beta x \pmod{1+x+xx}$.

10. If ξ is a prime function mod. $(1+x+xx)$ and its determinant = D , then in general

$$\zeta^D \equiv \zeta \pmod{1+x+xx, \xi}$$

11. Quadratic, cubic residues Modulus...

12. If P is a cubic residue of ξ , then:

$$P^{\frac{1}{2}(D-1)} \equiv 1 \pmod{1+x+xx, \xi}.$$

REMARKS ON THE DEVELOPMENT OF "ON THE THEORY OF CUBIC RESIDUES"

Gauss has made the effort here to the communicate his third proof of the quadratic reciprocity of cubic residues. The first approach referred only to the domain of rational whole numbers and utilized the following fundamental idea:

If the prime number is $p \equiv 1 \pmod{3}$, then the congruence $x^3 \equiv 1 \pmod{p}$ has three different roots, among whose one differing from 1 will be called f . In the system, $p-1$ modulus p , all incongruent [to each other], and p are prime whole numbers, multiplied with the 3 numbers $1, f, f^2$ then form a group of the index $\frac{p-1}{3}$, for which we imagine selected from any one of the manifold possible types of systems of representation S , composed of the numbers $\alpha_1, \alpha_2, \dots, \alpha_{\frac{p-1}{3}}$. It is characteristic with these numbers, that no two indices i, k can exist for [which] the congruence $\alpha_i \equiv f^{\pm 1} \alpha_k$ [holds]. If one designates the remaining systems S' and S'' for the $\frac{p-1}{3}$ numbers β , and $\frac{p-1}{3}$ numbers γ by

$$\beta_i \equiv f \alpha_i, \quad \gamma_i \equiv f^2 \alpha_i$$

then the $(p-1)$ numbers α, β, γ immediately exhaust the whole system of residues $1, 2, \dots, p-1 \pmod{p}$.

If a is any number not divisible by p , then

$$a^{\frac{p-1}{3}} \equiv f^2 \equiv \left[\frac{a}{p} \right] \pmod{p}$$

is the *cubic character* of a in the basis of p , and it [the character] is thus $\lambda = 0, 1$ or 2 .

To obtain a theorem concerning these cubic residues, one forms the $\frac{p-1}{3}$ products $a\alpha_1, a\alpha_2, \dots, a\alpha_{\frac{p-1}{3}}$. These numbers evidently again form a system of representation, since from the congruence $a\alpha_i \equiv f^{\pm 1} a\alpha_k$ would follow $\alpha_i \equiv f^{\pm 1} \alpha_k$. If now μ among the numbers $a\alpha_i$ belongs to the system S' , ν to the system S'' , then evidently their product mod p is congruent with $f^{\mu+2\nu} \cdot \alpha_1 \alpha_2 \dots \alpha_{\frac{p-1}{3}}$ obtains thus the result:

$$\left[\begin{array}{c} a \\ p \end{array} \right] \equiv a^{\frac{p-1}{3}} \equiv f^{\mu+3\nu} / p \pmod{p}$$

which is sufficiently analogous to the known lemma, which GAUSS laid out as the foundation in his third proof of the theorem of quadratic reciprocity.

Gauss' own arguments refers to a special classification of the $(p - 1)$ residues of mod. p into three classes S , S' and S'' , whereby the representation of p in the form $(mm+3nn)$ is used. However, most likely the intricacies which are associated with this denotation of the number f have been left out by Gauss, [of which I (?)] here proceed in the previous way. In fact, in this place, the necessity of the development of the domain of numbers[zahlgebiet] from complex whole numbers $(a + b\rho)$, where thereby instead of f the roots of 1 $\rho = \frac{-1+i\sqrt{3}}{2}$ completes itself, will be quite particularly convincing.

In any case, the relevant investigations had been carried out in the time before 1809, and were likely directly associated with mentioned developments in quadratic residues, which were submitted in January 1806 to the Goettingen Academy of the Sciences. According to notes in a daybook ¹ of Gauss's, conducted since the end of March 1796 during a longer series of years of his investigation, the same detailed [notes] on the theory of cubic and biquadratic residues middle is published in mid February 1807. There again however the replacement of f by ρ is likely directly associated to it, as arises out of the original of the here preceding communicated note. Thus, one may assume that Gauss definitely already had carried out around the designated time (1808) the following series step/iteration of the implementation of the whole complex numbers.

Gauss had also assembled the three classes S , S' and S'' for the complex prime numbers $2 - \rho$ and $3 - \rho$ (the above are reproduced) likewise for the prime parts $3 - 2\rho$ of 19. Particularly interesting is that Gauss clothed this consideration in geometrical form(as also accordingly with the biquadratic residues). The whole complex numbers $a + b\rho$ yield points on the plane, which represent a rhombic point lattice. The point lattice of a single system S can thus contain an area, which (spoken in a new sense) can be understood as discontinuous areas of an infinite group of linear substitutions. Gauss has produced symbols for various cases; which is conveyed above for the prime number $6 - \rho$. In order to treat the group it would be:

$$u' = \rho^\nu u + (a + b\rho),$$

where u denotes a complex variable, set $\nu = 1, 2, 3$ and $a + b\rho$ all of the congruences

$$a + b\rho \equiv 0 \pmod{6 - \rho}$$

is to traverse sufficient whole numbers. The area in the cited Gaussian figure corresponds to the group extended by addition of the substitution $u' = \pm u$. The arbitrariness in the choice of the system of representation S now accumulates the arbitrariness of the choice of the area limits beyond. Which intent Gauss had observed in choosing the form of this limit is unfortunately not stated.

The twelve theses on the conclusions of the above note compiled under [2] follow directly in the original from the considerations of the numbers $a + b\rho$. The system of all whole complex numbers $a + b\rho$ clearly shows here the system of all whole functions of x with whole number coefficients reduced by replacement of the mod. $(1 + x + xx)$.

-FRICKE.

¹Particulars concerning this journal of highest value are made in book 9 of the collected works.