

# Appendix

Objektyp: **Appendix**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **21 (1975)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **13.09.2024**

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

A direct computation gives the following values

$$\begin{aligned} a &= 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \\ \Delta_a &= 4, -9, -1, -11, -1, 1, 11, 1, 9, -4 \end{aligned}$$

The fifth powers are  $4a = 1, 10$  that is  $a = 3, 8$  and for these  $\Delta_3 = (-3/p)_{\mathbf{Z}} \cdot x = -x = -1$  and  $\Delta_8 = (-8/p)_{\mathbf{Z}} \cdot x = x = 1$  as required.

I should like to thank Professor Frohlich sincerely for his suggestion to look at these  $\Delta_a$ .

### APPENDIX

1. For the convenience of the reader we give here the definition of  $(\alpha/\beta)_{10}$ , the tenth power residue symbol and some of its properties.

First let  $\pi$  be a prime factor of a rational prime  $p \equiv 1 \pmod{5}$ . The residue classes mod  $\pi$ , in  $\mathbf{Z}[\zeta]$ , form a field of norm  $\pi = p$  elements. The non-zero classes form a cyclic group (multiplicative)  $1, \rho, \dots, \rho^{p-2}$  of  $p - 1$  elements. This group has in it just 10 elements or order dividing 10 viz.  $\rho^{j(p-1)/10}$  ( $j = 0, 1, \dots, 9$ ). These are represented (mod  $\pi$ ) by  $\pm 1, \pm \zeta, \dots, \pm \zeta^4$ , since these are distinct mod  $\pi$  and have order dividing 10. Now let  $\alpha$  be any non-zero residue mod  $\pi$ . Then  $\alpha^{(p-1)/10}$  has order dividing 10 and so is congruent to one of  $\pm 1, \pm \zeta, \dots, \pm \zeta^4 \pmod{\pi}$ . We define  $(\alpha/\pi)_{10} = \pm 1, \pm \zeta, \dots, \pm \zeta^4$  according as  $\alpha^{(p-1)/10}$  is congruent to  $\pm 1, \pm \zeta, \dots, \pm \zeta^4 \pmod{\pi}$ . It follows that

$$(\alpha/\pi)_{10} \equiv \alpha^{(N\pi-1)/10} \pmod{\pi}.$$

It is immediately verified that  $(\alpha\beta/\pi)_{10} = (\alpha/\pi)_{10} \cdot (\beta/\pi)_{10}$ , and we define  $(\alpha/\pi_1\pi_2)_{10} = (\alpha/\pi_1)_{10} \cdot (\alpha/\pi_2)_{10}$ . The following properties may be easily verified directly from the definition.

(i). If  $p \equiv 2, 3 \pmod{5}$ , so that  $p$  stays prime in  $\mathbf{Z}[\zeta]$ , and if  $n \in \mathbf{Z}$ , then  $(n/p)_{10} = 1$ .

(ii). If  $\pi$  is a prime factor of a  $p \equiv 4 \pmod{5}$ , so that  $p = \pi \bar{\pi}$  is the prime decomposition of  $p$  in  $\mathbf{Z}[\zeta]$ , and  $n \in \mathbf{Z}$ , then

$$(n/\pi)_{10} = 1.$$

(iii). If  $\pi$  is a prime factor of a  $p \equiv 1 \pmod{5}$ , so that  $p = \pi_1 \pi_2 \bar{\pi}_2 \bar{\pi}_1$  is the prime decomposition of  $p$  in  $\mathbf{Z}[\zeta]$ , then

$$(n/\pi)_{10} \cdot (n/\bar{\pi})_{10} = 1.$$

(iv). If  $\pi$  is a complex prime factor of a  $p \equiv 1, 4 \pmod{5}$  and  $\sigma$  of a  $q \equiv 1, 4 \pmod{5}$ , then  $\overline{(\pi/\sigma)_{10}} = (\bar{\pi}/\bar{\sigma})_{10}$ .

2. The symbol  $(\alpha/\beta)_5$  is defined in the same way and has similar properties.

3. The symbol  $(a/p)_{\mathbf{Z}}$  is simply the ordinary Legendre symbol, the subscript  $\mathbf{Z}$  is used to distinguish it from the symbol  $(\alpha/\beta)_2$  which denotes the quadratic character of  $\alpha$  modulo  $\beta$  in a given ring, e.g. if  $\alpha, \beta \in \mathbf{Z}[i]$

$$\text{then } (\alpha/\beta)_{\mathbf{Z}[i]} = \begin{cases} 1 & \text{if } x^2 \equiv \alpha \pmod{\beta} \text{ is solvable in } \mathbf{Z}[i], \\ -1 & \text{otherwise.} \end{cases}$$

#### REFERENCES

- [1] DICKSON, L. E. Cyclotomy, higher congruences and Waring's problem. *American Journal of Mathematics*, 57 (1935), pp. 391-424.
- [2] RAJWADE, A. R. On rational primes  $p$  congruent to 1 (mod 3 or 5). *Proc. Camb. Phil. Soc.* 66 (1969), pp. 61-70.
- [3] ——— On the congruence  $y^2 \equiv x^5 - a \pmod{p}$ . *Proc. Camb. Phil. Soc.* (to appear).

(Reçu le 7 janvier 1975)

A. R. Rajwade

Department of Mathematics  
Panjab University  
Chandigarh, India