

## Calculs sur des modules finis 6

**Auteurs : Dedekind, Richard**

En passant la souris sur une vignette, le titre de l'image apparaît.

2 Fichier(s)

Contributeur·rices Haffner, Emmylou

Éditeurs Emmylou Haffner (Institut des textes et manuscrits modernes, CNRS-ENS) ; Niedersächsische Staats- und Universitätsbibliothek, Göttingen ; projet EMAN (Thalim, CNRS-ENS-Sorbonne nouvelle).

### Présentation

Titre Calculs sur des modules finis 6

Date 1892-3

Sujet

- modules
- modules finis
- théorie des nombres

Cote Cod. Ms. Dedekind X 9, p. 29

Format 1 f. ; 2 p.

Langue Allemand

### Description & Analyse

Description Suite des calculs de la page précédente.

Vers la fin de la page, question supplémentaire : Peut-être choisir  $q \bmod p$  tel quel  $q$  soit relativement premier à  $n$  ? Réponse au problème.

Mode(s) d'écriture

- Aufgaben
- Calculs phase 1

Auteur·es de la description Haffner, Emmylou

### Relations

**Collection Cod. Ms. Dedekind X 9**

*Ce document a les mêmes calculs que :*



[Calculs sur des modules finis 5](#)

Collection Cod. Ms. Dedekind X 9

[Calculs sur des modules finis 7](#) a les mêmes calculs que ce document

---

[Afficher la visualisation des relations de la notice.](#)

## Mots-clefs

[modules](#), [modules finis](#), [théorie des nombres](#)

Notice créée par [Emmylou Haffner](#) Notice créée le 24/10/2018 Dernière modification le 17/09/2020

---



$$r = [m\alpha, p\alpha + n\beta] = [am\alpha' + bm\beta', (cp + en)\alpha' + (bp + dn)\beta']$$

$$v = [\alpha, \beta] = [\alpha', \beta'] \quad \text{Man nehme ein } [m, n] = [1, 1]$$

$$\begin{cases} \alpha = a\alpha' + b\beta' \\ \beta = c\alpha' + d\beta' \\ ad - bc = 1 \end{cases}$$

Man nehme ein  $[m, n] = [1, 1]$   
 $[p, n] = n'$   
 so n\u00e4he man die relation  $bp + dn = n'$

$$\text{L\u00f6st } bp + dn = n' \quad b \frac{p}{n'} + d \frac{n}{n'} = 1$$

$$\begin{aligned} b \cdot bm + d \cdot (bp + dn) &= 1 \\ = b \cdot b'm + b \cdot d'p + d \cdot d'n &= 1 \\ = b(b'm + d'p) + d \cdot d'n &= 1 \end{aligned}$$

$$\begin{aligned} b &= b_0 + x \frac{n}{n'} \\ d &= d_0 - x \frac{p}{n'} \\ bm &= (b_0 + x \frac{n}{n'})m \quad , \quad n' \end{aligned}$$

$$[bm, n'] = [b, n'] \quad bp + dn = k + [p, n]$$

Ersetzt man in durch  $p, m, p$  durch  $p_2, m_2$   $b \frac{p}{n'} + d \frac{n}{n'} = 1$

$$r = [p_2 m_2, p_2 m_2 + n_2 \beta] ; [p_2, p_2] = [m_2, n_2] = 1$$

$$[b p_2 m_2, b p_2 m_2 + d n_2] = [b m_2, b p_2 m_2 + d n_2, d m_2 + d p_2 n_2]$$

$$\begin{aligned} p_2 p_2 + p_2 p_2 &= 1 &= [d p_2 p_2 n_2, d n_2 - d n_2 p_2 p_2, d m_2 + d p_2 n_2] \\ &= [d p_2 m_2, b m_2 + d p_2 n_2] \end{aligned}$$

$$\begin{aligned} b p_2 m_2 + d p_2 p_2 + d n_2 &= 1 \\ &= [b p_2 m_2, d p_2 m_2, b p_2 m_2 + d p_2 n_2, b m_2 + d p_2 n_2] \end{aligned}$$

Man nehme  
 f\u00fcr  $b$  den  
 gr\u00f6\u00dften gemeinsamen  
 Teiler von  
 $m_2, p_2$   
 so ist  $b$  rel. prim.  
 zu  $n_2$ . also  
 $\exists m, p, x, y \in \mathbb{Z}$

$$r = c [p m, q m \alpha + n \beta] ; [p, q] = [m, n] = 1$$

$$c [c m n - c q m v, c p m v, c^2 p m n] = [c^2 p m n]$$

$$c [m n - q m v, p m v, c p m n] = [c p m n]$$

Kann man  $q$  (mod.  $p$ ) so w\u00e4hlen, dass  $q$  relativ prim zu  $n$  wird?

$$q' = q + x p \text{ soll relativ prim zu } n \text{ werden!}$$

ist  $n'$  das Produkt aller diejenigen in  $n$  aufgehenden Primzahlen,  
 welche nicht in  $p$  aufgehen

Man nehme  $x, y$  mit den Zahlen  $m', n', n'$

$$m m' + p p' + n n' = 1 \quad \text{oder } x p + y n = 1$$

$$p z + n y = k \quad p z u + n y v + m n = 1$$

$$k x + m v = 1$$