

# Sätze zur Zahlentheorie

1. Die Eulersche  $\varphi$ -Funktion  $\varphi(m)$  ist die Anzahl der relativ primen Restklassen mod  $m$ . Gilt für  $m$  die kanonische Zerlegung  $m = \prod_{l=1}^r p_l^{\alpha_l}$  ( $\alpha_l \in \mathbb{N}$ ) so ist  $\varphi(m) = m \prod_{l=1}^r \left(1 - \frac{1}{p_l}\right)$   
 ist  $(a, b) = 1 \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$   
 Sonderfall:  $\varphi(p) = p - 1$  für alle Primzahlen  $p$

2. Kleiner Satz von Fermat:  
 Wenn  $(a, b) = 1$ , gilt  $a^{\varphi(b)} \equiv 1(b)$   
 Sonderfall:  $a^{p-1} \equiv 1(p)$

3. Satz von Wilson: „ $(m - 1)! \equiv -1(m)$ “ ist gleichbedeutend mit „ $m$  ist eine Primzahl“

4. Für alle Nichtprimzahlen gilt:  $n \mid (n - 1)!$ , falls  $n > 5$

5. Jede Primzahl  $p \equiv 1(4)$  lässt sich eindeutig als Summe zweier Quadrate darstellen.  $p = a^2 + b^2$  mit  $(a, b) = 1$   
 Gilt  $p \mid n$  mit  $n = a^2 + b^2$  und  $(a, b) = 1$ , so ist  $p = 2$  oder  $p \equiv 1(4)$   
 Es gibt unendlich viele Primzahlen  $\equiv 1(4)$

6. Dirichletscher Primzahlsatz:  
 In jeder arithmetischen Folge  $a_n = l + nk$  mit  $l, k \in \mathbb{N}$ ,  $(l, k) = 1$ ,  $n = 1, 2, \dots$  gibt es unendlich viele Primzahlen.

7. Es gibt unendliche viele natürlichen Zahlen  $n$ , die keine Primzahlen sind und für die gilt:  $2^{n-1} \equiv 1(n)$

8. Primfaktorenzerlegung von  $n!$  mit  $n = \prod_{l=1}^k p_l^{\alpha_l}$

$$n! = \prod_{p \leq n} p^{\left(\sum_{l=1}^{\infty} \left\lfloor \frac{n}{p^l} \right\rfloor\right)}$$

9.  $a^n - b^n$  bzw.  $a^n + b^n$  ( $1 \leq b < a$ ,  $(a, b) = 1$ ,  $a, b \in \mathbb{N}$ ) ist höchstens dann eine Primzahl, wenn  $n = p$  und  $a - b = 1$ , bzw.  $n = 2^k$

10. Sei  $p_n$  die  $n$ -te Primzahl ( $n > 6$ ). Dann gilt  $2n + 1 < p_n < 2^{2^{n-2}}$

11. Paarweise teilerfremde natürliche Zahlen  $x, y, z$  sind genau dann pythagoräisch ( $x^2 + y^2 = z^2$ ), wenn mit  $a, b \in \mathbb{N}$ ,  $a > b$ ,  $(a, b) = 1$ ,  $a \neq b(2)$  gilt:

$$x = a^2 - b^2, y = 2ab, z = a^2 + b^2 \quad (\text{indische Formeln})$$

12. Pellische Gleichung:  
 $x^2 = ay^2 + 1$  in  $\mathbb{Z} \times \mathbb{Z}$  lösen. Wenn  $a = g^2 \pm 2 \Rightarrow x^2 = g^2 \pm 1, y = g$ ; wenn  $a = g^2 \pm 1 \Rightarrow x = 2g^2 \pm 1, y = 2g$  ( $g \in \mathbb{Z}$ ).  
 Allgemein: Ist  $(m_0 \mid n_0)$  eine Lösung, so ist auch  $(m_1 \mid n_1)$  Lösung mit  $m_1 = m_0^2 + an_0^2, n_1 = 2m_0n_0$ .

13. Für  $n \geq 2$  gilt:  $p_{n+1} < 2p_n$   $p_n \dots n$ -te Primzahl

14. Sei  $\Pi(x) = \sum_{p \leq x} 1$  die Anzahl aller Primzahlen  $\leq x$ . Dann gilt:  $\Pi(x) > \ln(\ln x)$  für  $x \geq 3$

15. Gaußscher Primzahlsatz:  $\lim_{x \rightarrow \infty} \Pi(x) \cdot \frac{\ln x}{x} = 1$   
 insbesondere:  $\frac{1}{6} < \frac{\ln x}{x} (\Pi(2x) - \Pi(x)) < \frac{7}{5}$  für  $x \geq 2$ .

16. Stirlingsche Formel:

$$n! = n^n \cdot e^{-n} \cdot \sqrt{2\pi n} \cdot e^{\frac{\beta_n}{12n}} \quad (0 \leq \beta_n \leq 1)$$

17. Sind  $F_\nu$  Fermatsche Zahlen, so gilt:  $(F_n, F_m) = 1$ , falls  $n \neq m$   
 $F_\nu = 2^{(2^\nu)} + 1 \quad \nu \in \mathbb{N}_0$

18.  $\sigma_0(n)$  ist die Anzahl der Teiler von  $n$ . Gilt  $n = \prod_{l=1}^r p_l^{\alpha_l}$ , so ist  $\sigma_0(n) = \prod_{l=1}^r (\alpha_l + 1)$  und  $\prod_{t|n} t = n^{\frac{\sigma_0(n)}{2}}$  und  $\sigma_0(n) = \sum_{l=1}^{\infty} (\lfloor \frac{n}{l} \rfloor - \lfloor \frac{n-1}{l} \rfloor)$ ,  $\sigma_0(p) = 2$  für alle Primzahlen  $p$ .  $\sigma_1(n) = \sum_{t|n} t$  mit  
 $\sigma_1(n) = \prod_{l=1}^r \frac{p_l^{\alpha_l+1} - 1}{p_l - 1}$

19. Ist  $(a, m) = 1$  und für  $a$  sei  $e(a)$  die kleinste natürliche Zahl, für die  $a^{e(a)} \equiv 1(m)$  gilt, so heißt  $e(a)$  der Exponent von  $a$  mod  $m$ . Es gilt:  $e(a) \mid \varphi(m)$ . Ist  $a^n \equiv 1(m) \Rightarrow e(a) \mid n \quad (n \in \mathbb{N})$

20.  $a$  heißt Primitivwurzel mod  $p$  (für Primzahlen  $p$ ), wenn die kleinsten positiven Reste von  $a^k$  ( $k = 1, \dots, p-1$ ) genau die Zahlen  $\{1, 2, \dots, p-1\}$  je einmal ergeben. Die Anzahl der Primitivwurzeln mod  $p$  ist  $\varphi(\varphi(p)) = \varphi(p-1)$ .  
 Damit  $a$  Primitivwurzel mod  $p$  ist, ist notwendig, dass  $a^{\frac{p-1}{2}} \equiv -1(p)$  ist. ( $p > 2$ )  
 PW(2)=1

21. In der rational gekürzten Zahl  $\frac{r}{s}$  ( $0 < r < s$ ) sei  $v$  die Länge der Vorperiode und  $l$  die Länge der Periode in der Dezimalschreibweise. Es gilt: wenn  $s = 2^a \cdot 5^b \cdot q$  mit  $(q, 10) = 1$  ist, so ist  $v = \max(a, b)$  und  $l = e(10) \bmod q$

22. Chinesischer Restsatz:

Seien  $m_1, m_2, \dots, m_k$  paarweise teilerfremde natürliche Zahlen und  $a_1, a_2, \dots, a_k$  beliebige natürliche Zahlen. Dann besitzt das simultane Kongruenzsystem

$$\begin{cases} x \equiv a_1(m_1) \\ x \equiv a_2(m_2) \\ \vdots \\ x \equiv a_k(m_k) \end{cases} \quad \text{genau eine Lösung } x_0 \bmod M \quad M = \prod_{i=1}^k m_i$$

Berechnung von  $x_0$ :

Sei  $M_l = \frac{M}{m_l}$  und  $M_l \equiv \overline{M}_l(m_l)$  mit  $0 < \overline{M}_l < m_l$  und sei  $\overline{m}_l$  die Lösung der Kongruenz  $x \cdot \overline{M}_l \equiv 1(m_l)$ , dann ist  $x_0 = \sum_{l=1}^k M_l \overline{m}_l a_l$

23. Ist mit  $c \in \{0, 1, \dots, m-1\}$  die Kongruenz  $x^2 \equiv c(m)$  lösbar bzw. nicht lösbar, so heißt  $c$  quadratischer Rest bzw. quadratischer Nichtrest mod  $m$ . Die quadratischen Reste  $a$  mod  $p$  ( $p > 2$ ,  $p$  Primzahl) lösen die Kongruenz  $x^{\frac{p-1}{2}} \equiv 1(p)$ , während die quadratischen Nichtreste  $a$  die Kongruenz  $x^{\frac{p-1}{2}} \equiv -1(p)$  lösen.

24. Legendre-Symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest mod } p \\ -1 & \text{falls } a \text{ quadratischer Nichtrest mod } p \\ 0 & \text{falls } a \equiv 0(p) \end{cases} \quad (p \text{ Primzahl})$$

Es gilt:

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}, \quad \left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv \pm 1(8) \\ -1 & \text{falls } p \equiv \pm 3(8) \\ 0 & \text{falls } p = 2 \end{cases} \quad \left(\frac{-1}{p}\right) = \pm 1 \text{ f\"ur } p \equiv \pm 1(4)$$

25. Gaußscher Reziprozitätssatz: Für ungerade Primzahlen  $p, q$  ( $p > q$ ) gilt:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

26. Satz von Liouville:

Ist  $\zeta$  eine algebraische Zahl  $n$ -ten Grades ( $n > 1$ ), so gibt es ein  $c \in \mathbb{R}^+$  derart, dass die Ungleichung  $\left|\zeta - \frac{p}{q}\right| < \frac{c}{q^n}$  keine Lösung mit ganzen Zahlen  $p, q$  ( $q > 0$ ) hat. Berechnung von  $c$ : Seien  $\zeta_\nu$  ( $\nu = 1, \dots, n$ ) die (komplexen) Lösungen der Gleichung  $a_n x^n + \dots + a_0 = 0$  ( $a_\nu \in \mathbb{Z}, a_n \neq 0$ )  $\zeta_1 = \zeta$ , so wird die Zahl  $M$  so gewählt, dass gilt:  $M > \max_\nu (1, |\zeta_\nu|)$ . Dann kann  $c$  beliebig gewählt werden mit  $0 < c < \min\left(M, \frac{1}{|a_n|}, (3M)^{1-n}\right)$

27. Betrand'sches Postulat: Für alle  $n \in \mathbb{N}$  mit  $n > 1$  gibt es eine Primzahl  $p$ , sodass  $n < p < 2p$  ist.