Zahlentheorie

Grundlagen der theoretischen Informatik

Übung 11

2021

Kongruenz.

Zwei ganze Zahlen a und b sind kongruent modulo m (in Zeichen $a \equiv b \pmod{n}$), wenn $m \mid b - a$ gilt, wobei m eine positive, ganze Zahl ist.

Eigenschaften von Kongruenzen.

(i) $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \quad \Rightarrow \quad a + c \equiv b + d \pmod{m}$

(ii) $a \equiv b \pmod{m},\ c \equiv d \pmod{m} \quad \Rightarrow \quad ac \equiv bd \pmod{m}$

(iii) $a \equiv b \pmod{m} \quad \Leftrightarrow \quad ac \equiv bc \pmod{mc}$

(iv) $ad \equiv bd \pmod{m} \quad \Leftrightarrow \quad a \equiv b \left(\frac{m}{\mathrm{ggT}(m,d)}\right)$

Satz (Lösbarkeit von linearen Kongruenzen).

Die Kongruenz $ax \equiv b \pmod{m}$ ist genau dann lösbar, wenn $\mathrm{ggT}(a, m) \mid b$ gilt.

Ist die Kongruenz lösbar, dann gibt es $\mathrm{ggT}(a, m)$ Lösungen. (Die Lösungen bilden eine arithmetische Progression mit Differenz $m/\mathrm{ggT}(a, m)$.)

Die eulersche Phi-Funktion.

Für jede positive, ganze Zahl n bezeichnet $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen in $\{1, \ldots, n\}$.

Die Berechnungsformel der eulerschen Phi-Funktion.

Hat eine ganze Zahl $n > 1$ die kanonische Primfaktorzerlegung $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, so gilt

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

Satz von Euler-Fermat.

Für alle $a \in \mathbb{Z}$ und $n \in \mathbb{Z}^+$ mit $\mathrm{ggT}(a, n) = 1$ gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Der kleine fermatsche Satz (erste Form).

Für jede $a \in \mathbb{Z}$ und für jede Primzahl p mit $p \nmid a$ gilt

$$a^{p-1} \equiv 1 \pmod{n}.$$

Der kleine fermatsche Satz (zweite Form).

Für jede $a \in \mathbb{Z}$ und für jede Primzahl p gilt

$$a^{p} \equiv a \pmod{n}.$$

1. Für welche Primzahlen p
   (a) sind die Zahlen $p+10$ und $p+14$ auch Primzahlen;
   (b) ist die Zahl p^2+2 auch eine Primzahl;
   (c) sind die Zahlen p^2+4 und p^2+6 auch Primzahlen?
2. Bestimmen Sie mit dem euklidischen Algorithmus die folgenden größten gemeinsamen Teiler:
   (a) $\mathrm{ggT}(13, 28)$;
   (b) $\mathrm{ggT}(899, 493)$;
   (c) $\mathrm{ggT}(612, 834)$.
3. Bestimmen Sie die Teileranzahlen von $10!$ und $\binom{12}{6}$.
4. Bestimmen Sie die minimale Teileranzahl einer Zahl n, wenn die Teileranzahl von n^2 gleich 143 ist.
5. Lösen Sie die folgenden linearen Kongruenzen.
   (a) $3x \equiv 2 \pmod 5$
   (b) $4x \equiv 6 \pmod{10}$
   (c) $10x \equiv 7 \pmod{100}$
   (d) $13x \equiv 1 \pmod{28}$
   (e) $66x \equiv 24 \pmod{36}$
6. Bestimmen Sie die folgenden Werte der eulerschen Phi-Funktion: $\varphi(60)$, $\varphi(100)$, $\varphi(11)$.
7. Bestimmen Sie den Rest
   (a) von 5^{2017} nach der Division durch 17;
   (b) von 108^{182} nach der Division durch 19;
   (c) von $73^{37} + 37^{73}$ nach der Division durch 108;
   (d) von $46^{47^{48}}$ nach der Division durch 25;
   (e) von $42^{41^{40}}$ nach der Division durch 121.
8. Beweisen Sie, dass
   (a) $4^{24} - 3^{24}$ durch 35 teilbar ist;
   (b) $1010^{1343} - 2$ durch 2019 teilbar ist (die Primfaktorzerlegung von 2019 ist $2019 = 3 \cdot 673$).
9. Der Nikolaus verteilt Salonzucker unter den 368 Erstsemestlern des Elektroingenieurwesens. Jeder Student, der die Klausuraufgabe über den Nikolaus lösen konnte, erhält 17 Stücke Salonzucker, alle anderen Studenten erhalten 10 Stücke Salonzucker. Der Nikolaus bewahrt den Salonzucker in Packungen von 500 Stücken auf, und er öffnet nur so viele wie nötig. Nachdem der Nikolaus alle Studenten Salonzucker ausgeteilt hat, bleiben in der letzten Packung noch 5 Stücke übrig, die von den Krampi aufgegessen wurden. Wie viele Studenten haben die entsprechende Aufgabe gelöst?
10. Beweisen Sie die folgende Aussage: Eine Zahl $a = a_n a_{n-1} \dots a_1 a_0$ ist genau dann durch 7 teilbar, wenn $a_n a_{n-1} \dots a_1 - 2a_0$ durch 7 teilbar ist.