Zahlentheorie

Lisa Sauermann

März 2013

Hier sollen einige grundlegende Lösungsmethoden für Zahlentheorieaufgaben bei Olympiaden und anderen Wettbewerben vermittelt werden.

Der Chinesische Restsatz

Satz 1 *Seien m_1, m_2, ..., m_k teilerfremde positive ganze Zahlen und $M = m_1 \cdot m_2 \cdots m_k$ deren Produkt.*
Für ganze Zahlen n_1, n_2, ..., n_k gibt es genau eine ganze Zahl z mit $0 \leq z < M$ mit

$$z \equiv n_1 \pmod{m_1}$$
$$z \equiv n_2 \pmod{m_2}$$
$$z \equiv n_k \pmod{m_k}$$

Beweis: Wir zeigen zuerst, dass es mindestens ein solches z gibt. Es ist $M_1 = m_2 \cdot m_3 \cdots m_k$ zu m_1 teilerfremd. Wir wissen, dass $m_2 \cdot m_3 \cdots m_k$ damit ein Inverses modulo m_1 hat, d. h. es gibt eine ganze Zahl a_1 mit $a_1 \cdot M_1 \equiv 1 \pmod{m_1}$.
Analog ist $M_i = \frac{M}{m_i}$ eine positive ganze Zahl und es gibt eine ganze Zahl a_i mit $a_i \cdot M_i \equiv 1 \pmod{m_i}$, $i = 2, \ldots, k$.
Nun wähle z mit $0 \leq z < M$ so, dass

$$z \equiv n_1 \cdot a_1 \cdot M_1 + n_2 \cdot a_2 \cdot M_2 + \cdots + n_k \cdot a_k \cdot M_k \pmod{M}$$

gilt. Da M_j für $j \neq i$ durch m_i teilbar ist, ergibt sich $M_j \equiv 0 \pmod{m_i}$ für $j \neq i$ und damit

$$z \equiv n_i \cdot a_i \cdot M_i \equiv n_i \cdot 1 \pmod{m_i}.$$

Damit erfüllt dieses z die Bedingungen.
Angenommen, es gäbe $z > z'$, die beide die Bedingungen erfüllen. Dann gilt $z - z' \equiv n_i - n_i \equiv 0 \pmod{m_i}$ für alle $1 \leq i \leq k$. Weil die m_i paarweise teilerfremd sind, folgt daraus $z - z' \equiv 0 \pmod{M}$. Das ist aber ein Widerspruch zu $1 \leq z - z' < M$.
Damit gibt es genau ein solches z. $\square$
Der Chinesische Restsatz ist sehr wichtig und nützlich. Mit ihm allein kann man die folgende IMO-Aufgabe lösen.

Aufgabe 1 (5. Aufgabe der IMO 1989) Für welche positiven ganzen Zahlen n gibt es eine positive ganze Zahl N, sodass keine der Zahlen $1+N$, $2+N$, $\dots$, $n+N$ eine Potenz einer Primzahl ist?

Die φ- und die τ-Funktion

Für eine positive ganze Zahl n sei mit $\varphi(n)$ die Anzahl der zu n teilerfremden positiven ganzen Zahlen $\leq n$ bezeichnet. Beispielsweise gilt $\varphi(1)=1$, $\varphi(3)=2$ und $\varphi(6)=2$.
Für eine Primzahlpotenz p^m (mit p prim, $m \geq 1$ ganz) gilt $\varphi(p^m) = p^m - p^{m-1}$. Denn es sind genau die Zahlen zu p^m teilerfremd, die zu p teilerfremd sind und es gibt genau $p^m \cdot \frac{p-1}{p} = p^m - p^{m-1}$ nicht durch p teilbare positive ganze Zahlen $\leq p^m$.
Für zueinander teilerfremde positive ganze Zahlen m, n gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$. Denn nach dem Chinesischen Restsatz gibt es für jedes Paar von Resten modulo m und n genau einen entsprechenden Rest modulo mn. Damit gibt es für jedes der $\varphi(m) \cdot \varphi(n)$ Paare eines jeweils teilerfremden Restes modulo m und n genau einen entsprechenden Rest modulo mn. Dies sind aber genau die $\varphi(m \cdot n)$ zu $m \cdot n$ teilerfremden Reste.
Sei nun allgemein $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ $(a_1, \dots, a_k \geq 1)$ eine beliebige natürliche Zahl in ihrer Primfaktorenzerlegung. Dann gilt

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \cdot \ldots \cdot \varphi(p_k^{a_k}) \\ &= \left(p_1^{a_1} - p_1^{a_1-1}\right) \cdot \left(p_2^{a_2} - p_2^{a_2-1}\right) \cdot \ldots \cdot \left(p_k^{a_k} - p_k^{a_k-1}\right) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

Im Satz von Euler-Fermat wird die φ-Funktion noch eine wichtige Rolle spielen. Nach ihrem Entdecker wird sie oft auch Eulersche φ-Funktion genannt.
Für eine positive ganze Zahl n sei mit $\tau(n)$ die Anzahl der positiven Teiler von n bezeichnet. Beispielsweise gilt $\tau(1)=1$, $\tau(3)=2$ und $\tau(6)=4$.
Sei nun allgemein $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ eine beliebige natürliche Zahl in ihrer Primfaktorenzerlegung. Dann hat jeder Teiler von n die Form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ mit $b_i \leq a_i$ für $1 \leq i \leq k$. Damit gibt es für b_i jeweils a_i+1 Möglichkeiten (nämlich $0, 1, 2, \dots a_i$). Insgesamt beträgt die Anzahl der Teiler von n also

$$\tau(n) = (a_1+1)(a_2+1)\cdots(a_k+1).$$

Diese sehr nützliche Formel erschlägt die folgende Aufgabe sofort. Nicht ganz so leicht ist dagegen Aufgabe 3.

Aufgabe 2 Gibt es eine dreistellige Zahl mit genau 11 Teilern (im Dezimalsystem)?

Aufgabe 3 (431046) Beweise: Bei jeder natürlichen Zahl n, bei der $n+1$ durch 24 teilbar ist, ist auch die Summe aller Teiler von n durch 24 teilbar.

Der Satz von Euler-Fermat

Satz 2 *Sei m eine positive ganze Zahl und a eine zu ihr teilerfremde ganze Zahl. Dann gilt*

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

Beweis: Es seien $x_1 = 1, x_2, \dots, x_{\varphi(m)}$ die zu m teilerfremden ganzen Zahlen von 1 bis m. Nun sind auch $a\,x_1, a\,x_2, \dots, a\,x_{\varphi(m)}$ zu m teilerfremd. Wegen $x_j \not\equiv x_i \pmod{m}$ gilt $a\,x_j \not\equiv a\,x_i \pmod{m}$ für $1 \le i < j \le \varphi(m)$. Damit haben die zu m teilerfremden Zahlen $a\,x_1, a\,x_2, \dots, a\,x_{\varphi(m)}$ paarweise verschiedene Reste. Es gibt aber nur die $\varphi(m)$ zu m teilerfremden Reste $x_1, x_2, \dots, x_{\varphi(m)}$. Damit sind die Reste von $a\,x_1, a\,x_2, \dots, a\,x_{\varphi(m)}$ und $x_1, x_2, \dots, x_{\varphi(m)}$ bei Teilung duch m bis auf die Reihenfolge gleich. Also gilt

$$a^{\varphi(m)} \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)} \equiv a\,x_1 \cdot a\,x_2 \cdots a\,x_{\varphi(m)} \equiv x_1 \cdot x_2 \cdot \ldots \cdot x_{\varphi(m)} \pmod{m}.$$

Daraus folgt $a^{\varphi(m)} \equiv 1 \pmod{m}$, da $x_1 \cdot x_2 \cdots x_{\varphi(m)}$ teilerfremd zu m ist und deshalb auf beiden Seiten der Kongruenz gekürzt werden kann. □

Ein bekannter Spezialfall des Satzes von Euler-Fermat ist der kleine Satz von Fermat: Für eine Primzahl p und eine nicht durch diese teilbare Zahl a gilt $a^{p-1} \equiv 1 \pmod{p}$.

Die Identität von Sophie Germain

Es gilt für beliebige ganze Zahlen a, b

$$a^4 + 4\,b^4 = \left(a^2 + 2b^2\right)^2 - 4\,a^2\,b^2 = \left(a^2 - 2\,a\,b + 2\,b^2\right)\left(a^2 + 2\,a\,b + 2\,b^2\right) .$$

Aufgabe 4 (380942) In einem Zahlensystem mit der Basis a ($a \in \mathbb{N}$, $a > 1$) sei die Zahl $z = 100\,000\,004$ gegeben. Beweise, dass es keine natürliche Zahl a gibt, für die z eine Primzahl ist.

Potenzreste

Aufgabe 5 (400941)

(a) Beweise: Für jede natürliche Zahl ist ihr Quadrat entweder von der Form $4k$ oder von der Form $8\,k + 1$, wobei jeweils k eine natürliche Zahl ist.

(b) Gibt es eine n-stellige Quadratzahl mit $n > 1$, die aus lauter gleichen Ziffern besteht? Beweise deine Antwort.

Diese recht einfache Aufgabe regt dazu an, sich mit den möglichen Resten von Quadratzahlen oder höheren Potenzen bei der Teilung durch bestimmte Zahlen zu befassen.

Durch Ausprobieren für alle Restklassen können wir uns leicht überlegen, welche Reste Quadratzahlen modulo 4 und 8 lassen können. Das Ergebnis ist durchaus interessant und wurde ja schon in Teil (a) der obigen Aufgabe verraten.

Auch die möglichen Reste von Quadratzahlen modulo 3, 9, 5 und 7 sollte man als Olympaideteilnehmer immer im Kopf haben. Bei vielen Aufgaben kann man aus den möglichen Resten modulo einer geschickt gewählten Primzahl nämlich bedeutende Schlüsse ziehen. Die folgenden Aufgaben sollen dies verdeutlichen.

Aufgabe 6 (420944) Ermittle alle diejenigen Tripel (a, b, c) ganzer Zahlen, für die die Gleichung $2\,a^2 + b^2 = 5\,c^2$ gilt.

Aufgabe 7 Ermittle alle diejenigen Paare (a, b) ganzer Zahlen, für die die Gleichung $a^5 = b^2 + 4$ gilt.

Aufgabe 8 (N1 2002) Was ist die kleinste positive ganze Zahl t, sodass es ganze Zahlen $x_1, x_2, \ldots, x_t$ mit $x_1^3 + x_2^3 + \cdots + x_t^3 = 2002^{2002}$ gibt?

Aufgabe 9 (1. Aufgabe der IMO 1986) Die Menge $S = \{2, 5, 13\}$ hat die Eigenschaft, dass für alle $a, b \in S, a \neq b$ die Zahl $a\,b - 1$ keine Quadratzahl ist. Zeige, dass für jede nicht in S enthaltene positve ganze Zahl d, die Menge $S \cup \{d\}$ diese Eigenschaft nicht hat.

Aufgabe 10 (N1 2000) Finde alle positiven ganzen Zahlen $n \geq 2$, die folgende Bedingung erfüllen: Für alle a, b teilerfremd zu n gilt

$$a \equiv b \pmod{n} \quad \text{genau dann wenn} \quad a\,b \equiv 1 \pmod{n}\,.$$

Einschachtelung von Quadratzahlen

Im vorhergehenden Abschnitt haben wir gesehen, wie man durch Betrachtung von Restklassen ausschließen kann, dass eine bestimmte Zahl eine Quadratzahl ist. Eine andere Methode ist die Betrachtung der Vielfachheiten ihrer Primfaktoren in der Primfaktorenzerlegung.

Eine dritte sehr wichtige und oft benötigte Strategie zum Beweis, dass eine Zahl keine Quadratzahl ist, ist die folgende: Wir zeigen, dass unsere Zahl zwischen zwei aufeinanderfolgenden Quadratzahlen liegt. Damit kann sie selbst keine Quadratzahl sein. Oft muss man etwas rechnen, damit die Einschachtelung gelingt, aber der Aufwand lohnt sich.

Hier eine zwei Beispielaufgaben

Aufgabe 11 (480846) Ermittle alle geordneten Paare (a, b) positiver ganzer Zahlen, für die $a^2 + 3\,b$ und $b^2 + 3\,a$ Quadratzahlen sind.

Aufgabe 12 (471346) Man bestimme alle reellen Zahlen x, für welche die beiden Zahlen $4\,x^5 - 7$ und $4\,x^{13} - 7$ gleichzeitig Quadrate ganzer Zahlen sind.

Dezimalsystembasteleien

Bei einigen Aufgaben wird besonderes Augenmerk auf das Dezimalsystem gelegt. Bei den folgenden drei Aufgaben muss man geschickt Vielfache, deren Dezimaldarstellungen bestimmte Eigenschaften haben, konstruieren. Ein wichtiger Trick ist dabei der folgende: Für jede zu 10 teilerfremde natürliche Zahl n gibt es eine Zehnerpotenz 10^m, die Rest 1 bei Teilung durch n lässt (nach Euler-Fermat). Nun ist die Zahl $1 + 10^m + 10^{2m} + \cdots + 10^{(n-1)m}$ durch n teilbar und hat eine sehr praktische Dezimaldarstellung. Man kann sie nämlich mit irgendeiner m-stelligen Zahl multiplizieren und erhält deren Dezimaldarstellung n mal hintereinander. Oft kann man dadurch die gewünschten Eigenschaften erfüllen. Ist die Ausgangszahl n durch 2 oder 5 teilbar, muss man dies durch geschickte Wahl von m berücksichtigen.

Aufgabe 13 (BWM 2009 1. Runde) Eine positive ganze Zahl heiße Dezimal-Palindrom, wenn ihre Dezimaldarstellung $z_n \dots z_0$ mit $z_0 \neq 0$ spiegelsymmetrisch ist, d. h. wenn $z_k = z_{n-k}$ für alle $k = 0, \dots, n$ gilt. Zeige, dass jede nicht durch 10 teilbare ganze Zahl ein positives Vielfaches besitzt, das ein Dezimal-Palindrom ist.

Aufgabe 14 Man finde alle positiven ganzen Zahlen k mit folgender Eigenschaft: Jede Zahl, die durch Umkehren der Dezimaldarstellung eines Vielfachen von k entsteht, ist ebenfalls ein Vielfaches von k.

Aufgabe 15 (6. Aufgabe der IMO 2004) Wir nennen eine positive ganze Zahl alternierend, wenn ihre Dezimaldarstellung abwechselnd gerade und ungerade Ziffern hat. Finde alle positiven ganzen Zahlen, die ein alternierendes Vielfaches besitzen.

Weitere Aufgaben

Aufgabe 16 (410943) Bestimme den größten gemeinsamen Teiler aller Zahlen der Form $n^4 - 4\,n^2$ mit $n \in \{1, 2, 3, \dots\}$, welche auf Null enden.

Aufgabe 17 (441044) Man bestimme alle natürlichen Zahlen $n > 1$ mit folgender Eigenschaft: Für jeden Teiler $d > 1$ von n ist die Zahl $d - 1$ ein Teiler von $n - 1$.

Attribution Section

sauermann (März 2013): Für KoSemNet freigegeben.
graebe (2014-01-01): Nach den KoSemNet Regeln aufbereitet.