Satz von Wilson

Sei $p \in \mathbb{N} \setminus \{0,1\}$, dann gilt $(p-1)! \equiv -1 \,(\mathrm{mod} p) \Longleftrightarrow p \,\mathrm{prim}$

Beweis:

zu zeigen sind

(i) $(p-1)! \equiv -1 \,(\mathrm{mod} p) \Longrightarrow p$ **prim**

(ii) $(p-1)! \equiv -1 \,(\mathrm{mod} p) \Longleftarrow p$ **prim**

zu (i):

$(A \Rightarrow B) \models (\neg B \Rightarrow \neg A)$, also aus (i) $\models \neg(p\,\mathrm{prim}) \Rightarrow \neg((p-1)! \equiv -1(\bmod p)) \models p$ zusammengesetzt $\Rightarrow (p-1)! \not\equiv -1 \,(\mathrm{mod} p)$

Sei zunächst $p = r \cdot s$ eine zusammengesetzte Zahl, die keine Quadratzahl ist. O.B.d.A. können wir $1 < r < s \leq p-1$ annehmen und es gilt

$$(p-1)! = \prod_{i=1}^{p-1} i = \underbrace{r \cdot s}_{p} \cdot \prod_{i \in \{1,\ldots,p-1\} \setminus \{r,s\}} i \equiv 0 \neq -1 \,(\mathrm{mod} p)$$

Sei andernfalls $p = r^2$ eine Quadratzahl, dann gilt für $p = 4$: $(4-1)! = 3! = 6 \equiv 2 \,(\mathrm{mod} 4)$, und für $p > 4$ (und somit $r > 2$ und der Feststellung, dass $2 \cdot r < r^2 = p$):

$$(p-1)! = \prod_{i=1}^{p-1} i = \underbrace{2r \cdot r}_{2p} \cdot \prod_{i \in \{1,\ldots,p-1\} \setminus \{r,2r\}} i \equiv 0 \neq -1 \,(\mathrm{mod} p)$$

Randbemerkung: Wenn die Zahl 1 in der Definitionsmenge im obigen Satz zugelassen wäre, erhielten wir für $p = 1$: $(1-1)! = 0! = 1 \equiv 0 \,(\mathrm{mod} 1)$. Dies sieht zwar zunächst nach dem gewünschten Resultat aus; weil aber ebenso $-1 \equiv 0(\bmod 1)$ gilt, hat das Resultat einen Pferdefuß: 1 wäre als Primzahl zu klassifizieren.[1]

zu (ii):

p prim $\Rightarrow \mathbb{F}_p$ ist Primkörper $\Rightarrow \forall x \in \mathbb{F}_p \setminus \{0\} \, \exists! y \in \mathbb{F}_p : x \cdot y \equiv 1 \,(\mathrm{mod} p)$ "inverses Element der Multiplikation"[2]

Betrachten wir zunächst die Elemente in dem Primkörper $\mathbb{F}_p$, die zu sich selbst invers sind: Sei $x^{-1} = x$, dann $1 = x \cdot x^{-1} = x^2$, also $0 = x^2 - 1 = (x+1) \cdot (x-1)$. Daraus folgt $(x+1 = 0) \vee (x-1 = 0)$ und damit $(x = -1) \vee (x = 1)$.

[1] Wie so häufig in der Mathematik stellt man auch hier fest: Sonderfälle sind Definitionssache. Mit der "Primzahl 1" wäre dann aber z.B. die (bis auf Reihenfolge) eindeutige Primfaktorzerlegung von positiven natürlichen Zahlen nicht mehr möglich, weil 1 das neutrale Element der Multiplikation ist und damit beliebig häufig (auch null-mal) als Faktor auftreten dürfte.

[2] Die Notation ist ein wenig unsauber, da wir hier den Primkörper $\mathbb{F}_p$ direkt mit einem (zudem unspezifizierten) isomorphen Repräsentantensystem identifizieren. Formal korrekt wäre es, den jeweils implizit benutzten Isomorphismus zwischen $\mathbb{F}_p$ und Repräsentantensystem explizit zu verwenden. – Wir können die Elemente des Körpers $\mathbb{F}_p$ beispielsweise als diejenigen Äquivalenzklassen definieren, die bei der Partitionierung des Rings der ganzen Zahlen durch die Operation "ganzzahliger Rest der Division durch p" entstehen. Jedes beliebige Repräsentantensystem dieser Elemente verhält sich dann isomorph zu $\mathbb{F}_p$ und ist dann eine p-elementige Teilmenge von $\mathbb{Z}$. – Die Kongruenzrelation $\equiv$ gibt dann an, dass die von ihr verknüpften Elemente in einer gemeinsamen Äquivalenzklasse bezüglich der Operation "ganzzahliger Rest der Division durch p" liegen. Streng genommen müßten wir auch die mathematischen Operationen danach unterscheiden, auf (bzw. in) welchen Strukturen sie definiert sind.

Wir partitionieren die verbleibende Menge[3] der “nicht selbstinversen” Elemente $\{2, ..., p-2\}$ in zwei disjunkte gleichmächtige Teilmengen P_1, P_2, so dass gilt: $\forall x \in P_1 \exists y \in P_2 : y = x^{-1}$.

Dann aber gilt

$$(p-2)! = \prod_{i=2}^{p-2} i = (\prod_{x \in P_1} x) \cdot (\prod_{y \in P_2} y) \equiv \prod_{x \in P_1} \underbrace{x \cdot x^{-1}}_{\equiv 1} \equiv \prod_{x \in P_1} 1 \equiv 1 \,(\mathrm{mod} p)$$

also

$$(p-1)! = (p-2)! \cdot (p-1) \equiv -1 \,(\mathrm{mod} p)$$

□

Weitergehende Betrachtung

$$(p-1)! = \prod_{i=1}^{p-1} i = (\prod_{i=1}^{p-k} i)(\prod_{i=p-k+1}^{p-1} i) = (p-k)! \cdot \prod_{i=1}^{k-1} (p-i)$$

$$\prod_{i=1}^{k-1} (p-i) \equiv \prod_{i=1}^{k-1} (-i) \equiv (\prod_{i=1}^{k-1} -1) \cdot \prod_{i=1}^{k-1} i \equiv (-1)^{k-1} (k-1)! \,(\mathrm{mod} p)$$

Sei p eine ungerade Primzahl; damit folgt $-1 \equiv (p-1)! \equiv (p-k)! \cdot (-1)^{k-1}(k-1)! \,(\mathrm{mod} p)$ und daher

$$(p-k)! \cdot (k-1)! \equiv (-1)^k \,(\mathrm{mod} p)$$

Spezialisiert für $k := \frac{p+1}{2}$ ergibt sich $(-1)^{\frac{p+1}{2}} \equiv \frac{2p-(p+1)}{2}! \cdot \frac{p+1-2}{2}! \equiv \left(\frac{p-1}{2}!\right)^2 \,(\mathrm{mod} p)$.

Sei nun zusätzlich $p \equiv 1 \,(\mathrm{mod}\, 4)$; dies ist äquivalent $p+1 \equiv 2 \,(\mathrm{mod}\, 4)$, und damit ist in diesem Fall $\frac{p+1}{2}$ eine ungerade Zahl (weil $p+1$ dann zwar durch 2, nicht aber durch 4 teilbar ist) , womit $(-1)^{\frac{p+1}{2}} = -1$ folgt. Somit $\left(\frac{p-1}{2}!\right)^2 \equiv -1 \,(\mathrm{mod} p)$, also mit dem Legendresymbol ausgedrückt: $p \equiv 1 \,(\mathrm{mod} 4) \Rightarrow \left(\frac{-1}{p}\right) = 1$; -1 ist in diesem Falle also ein quadratischer Rest modulo p.

Satz von Euler-Fermat

Seien $a, n \in \mathbb{N}$ mit $\gcd(a, n) = 1$. Sei ferner $\varphi : \mathbb{N} \to \mathbb{N}$ mit $n \mapsto |\{x \in \mathbb{N} | x < n \wedge \gcd(x, n) = 1\}|$ (also $\varphi(n)$ definiert als die Anzahl der zu n teilerfremden[4] Zahlen aus dem Bereich $\{1, ..., n\}$), dann gilt

$$a^{\varphi(n)} \equiv 1 \,(\mathrm{mod} n)$$

[3] Es sei bemerkt, dass aufgrund der Körperaxiome $a = a \cdot 1 = a \cdot (a^{-1} \cdot (a^{-1})^{-1}) = (a \cdot a^{-1}) \cdot (a^{-1})^{-1} = 1 \cdot (a^{-1})^{-1} = (a^{-1})^{-1}$ gilt. Wenn wir das additive neutrale Element 0 und das multiplikative neutrale Element 1 sowie dessen additives Inverses -1 aus dem Körper entfernen, so erhalten wir entweder die leere Menge oder eine Struktur, die sich in zwei Äquivalenzklassen partitionieren läßt, deren Repräsentanten a und a^{-1} sind.

[4] Zwei (oder mehrere) Zahlen bezeichnet man als *teilerfremd*, wenn ihr größter gemeinsamen Teiler 1 ist. – Dies mag zunächst etwas verwirrend erscheinen, da man ja eigentlich von *primteilerfremden* Zahlen sprechen müßte. Anderseits ist eine Definition von Teilerfremdheit, die den trivialen Teiler 1 beinhaltet, reichlich sinnlos: Alle Zahlen sind per definitionem durch 1 teilbar und damit gäbe es bei einer solchen Definition keine teilerfremden Zahlen. (Ganz zu schweigen davon, dass der Begriff *Primteilerfremdheit* in Restklassen keinen Sinn ergibt!)

Beweis: Sei $b_1, b_2, b_3, ..., b_{\varphi(n)}$ eine Aufzählung dieser zu n teilerfremden Zahlen. Dann ist auch $c_1, c_2, c_3, ..., c_{\varphi(n)}$ mit $c_i := a \cdot b_i \bmod n$ eine solche Aufzählung (denn wegen $\gcd(a, n) = 1$ existiert das multiplikative Inverse a^{-1} und es gilt $c_i = c_j \iff a \cdot b_i \equiv a \cdot b_j \pmod{n} \iff a \cdot b_i \cdot a^{-1} \equiv a \cdot b_j \cdot a^{-1} \pmod{n} \iff b_i \equiv b_j \pmod{n} \iff b_i = b_j \iff i = j$).[5]

Da beide Aufzählungen die gleichen Zahlen umfassen und die Multiplikation assoziativ und kommutativ ist, gilt $\prod_{i=1}^{\varphi(n)} b_i = \prod_{i=1}^{\varphi(n)} c_i$. Ferner existieren wegen $\gcd(c_i, n) = 1$ die multiplikativen Inversen c_i^{-1}modulo n. Es folgt

$$1 \equiv \prod_{i=1}^{\varphi(n)} 1 \equiv \prod_{i=1}^{\varphi(n)} \underbrace{c_i \cdot c_i^{-1}}_{\equiv 1} \equiv \prod_{i=1}^{\varphi(n)} \underbrace{a \cdot b_i}_{\equiv c_i} \cdot c_i^{-1} \equiv a^{\varphi(n)} \cdot \prod_{i=1}^{\varphi(n)} b_i \cdot \prod_{i=1}^{\varphi(n)} c_i^{-1}$$

$$\equiv a^{\varphi(n)} \cdot \underbrace{\prod_{i=1}^{\varphi(n)} c_i}_{\text{mit } \prod b_i = \prod c_i} \cdot \prod_{i=1}^{\varphi(n)} c_i^{-1} \equiv a^{\varphi(n)} \cdot \prod_{i=1}^{\varphi(n)} \underbrace{c_i \cdot c_i^{-1}}_{\equiv 1} \equiv a^{\varphi(n)} \cdot 1 \equiv a^{\varphi(n)} \pmod{n}$$

□

Bemerkung: Bei einer näheren Betrachtung des obigen Beweises stellt man fest: Er läßt sich auf endliche abelsche Gruppen übertragen. – In einer endlichen abelschen additiven Gruppe $\mathbb{G}_+$ erhalten wir dann die Aussage $\underbrace{a + a + ... + a}_{|\mathbb{G}_+|\text{-mal}} = 0$ (0 sei das additive neutrale Element der Gruppe). In einer endlichen abelschen multiplikativen Gruppe $\mathbb{G}.$ gilt dann analog $\underbrace{a \cdot a \cdot ... \cdot a}_{|\mathbb{G}.|\text{-mal}} = 1$ (1 sei das multiplikative neutrale Element der Gruppe). – Speziell für Körper beachte man, dass dort die Operationen Additition und Multiplikation definiert sind. Der Körper beinhaltet also (üblicherweise) zwei abelsche Gruppen, wobei das additive neutrale Element des Körpers kein Element der multiplikativen Gruppe des Körpers ist (Division durch 0 ist undefiniert!). *Beispiel:* Der Körper $\mathbb{F}_p$ besteht aus p Elementen; die in diesem Körper eingebettete additive Gruppe besteht ebenfalls aus p Elementen; die in $\mathbb{F}_p$ eingebettete multiplikative Gruppe besteht aus $p - 1$ Elementen (allen Elementen des Körpers ohne die Null).

Korollar

$$p \text{ prim} \wedge \gcd(a, p) = 1 \Longrightarrow a^{p-1} \equiv 1 \pmod{p}$$

Da eine Primzahl p zu allen natürlichen Zahlen a mit $1 \leq a < p$ teilerfremd ist, erhalten wir $\varphi(p) := p - 1$ und damit den historischen älteren "Kleinen Fermatschen Satz" $a^{p-1} \equiv 1 \pmod{p}$ als Korollar aus dem obigen Satz.

Beispiel: Primzahltest

Wie man mit geeigneten Methoden nachrechnen kann, ist $2^{5893-1} \bmod 5893 = 4877$. Damit wissen wir, dass 5893 keine Primzahl sein kann, obwohl uns die Teiler (noch) nicht bekannt sind. Wäre 5893 nämlich eine Primzahl, dann wäre $2^{5893-1} \bmod 5893 = 1$ und dies ist nicht der Fall.

[5]Streng genommen müssen wir auch die Existenz des Inversen beweisen, anstatt sie hier einfach zu postulieren. Außerdem wäre zu anzumerken (und ggf. zu zeigen), dass das Produkt zweier Zahlen, die zu n teilerfremd sind, ebenfalls zu n teilerfremd ist. – Da die Aufzählungen der b_i bzw. c_i endlich sind, muß dann jedes c_i auch in der Aufzählung der b_i vorkommen.

Bemerkung:

Aus dem kleinen Fermatschen Satz läßt sich nicht schließen, dass eine Zahl prim sein muß, wenn $a^{p-1} \equiv 1 \pmod{p}$ gilt. Man beachte, dass eine solche Behauptung oben weder aufgestellt (noch bewiesen) wurde.[6] Als Gegenbeispiel sei die zusammengesetzte Zahl $11 \cdot 31 = 341$ genannt: $2^{341-1} \bmod 341 = 1$ und $\gcd(2, 341) = 1$ sind erfüllt.

Korollar

Für $a, b, n \in \mathbb{N}$ mit $\gcd(a, n) = 1$ gilt $a^b \equiv a^{b \bmod \varphi(n)} \pmod{n}$

Beweis Wir setzen $b_1 := \left\lfloor \frac{b}{\varphi(n)} \right\rfloor$ und $b_2 := b \bmod \varphi(n)$, dann ist $b = b_1 \cdot \varphi(n) + b_2$ und wir erhalten

$$a^b \equiv a^{b_1\varphi(n)+b_2} \equiv a^{b_1\varphi(n)} \cdot a^{b_2} \equiv (\underbrace{a^{\varphi(n)}}_{1})^{b_1} \cdot a^{b_2} \equiv a^{b_2} \equiv a^{b \bmod \varphi(n)} \pmod{n}$$

Beispiel: Bestimmung der letzten Dezimalziffer des Terms 7^{17^k}

Sei k eine beliebige natürliche Zahl. Es gilt[7] $7^{17^k} = 7^{(17^k)}$ und damit $7^{17^k} \equiv 7^{17^k \bmod \varphi(10)} \bmod 10$. Wie man leicht nachzählt, ist $\varphi(10) = 4$. Da $17 \equiv 1 \pmod{4}$, gilt $17^k \equiv 1^k \equiv 1 \pmod{4}$, somit $17^k \bmod 4 = 1$. Die letzte Dezimalziffer von 7^{17^k}ist daher immer die 7 (unabhängig davon, wie k auch immer gewählt wird).

[6] Aus mathematisch-formaler Sicht ist dem eigentlich nichts hinzuzufügen. Aus didaktischer Sicht erscheint es jedoch sinnvoll, mögliche Irrtümer auszuräumen: Jede Äquivalenz ist eine Implikation, aber nicht jede Implikation ist eine Äquivalenz!

[7] Bemerkung: $a^{b^c} := a^{(b^c)}$. Dies ist zwar letztendlich eine Notationssache, aber es macht auch wirklich Sinn, die Exponentiation rechtsassoziativ zu definieren. Betrachten sie z.B. den Term $a^{(0+b^c+0)}$, für den man die Notation a^{0+b^c+0} als unproblematisch empfinden würde. Warum sollte man dann diesen nicht zu a^{b^c} vereinfachen dürfen?