Prof. Dr. H. Brenner **Osnabrück WS 2016/2017**

Zahlentheorie

Vorlesung 14

Fermatsche Primzahlen

DEFINITION 14.1. Eine Primzahl der Form $2^s + 1$, wobei s eine positive natürliche Zahl ist, heißt *Fermatsche Primzahl*.

LEMMA 14.2. *Bei einer Fermatschen Primzahl $2^s + 1$ hat der Exponent die Form $s = 2^r$ mit einem $r \in \mathbb{N}$.*

Beweis. Wir schreiben $s = 2^k u$ mit u ungerade. Damit ist

$$2^{2^k u} + 1 \ = \ \left(2^{2^k}\right)^u + 1.$$

Für ungerades u gilt generell die polynomiale Identität (da -1 eine Nullstelle ist)

$$X^u + 1 \ = \ (X+1)\left(X^{u-1} - X^{u-2} + X^{u-3} - \ldots + X^2 - X + 1\right).$$

Also ist $2^{2^k} + 1 \geq 3$ ein Teiler von $2^{2^k u} + 1$. Da diese Zahl nach Voraussetzung prim ist, müssen beide Zahlen gleich sein, und dies bedeutet $u = 1$. □

Eine Fermatsche Primzahl ist nach diesem Lemma also insbesondere eine Fermat-Zahl im Sinne der folgenden Definition.

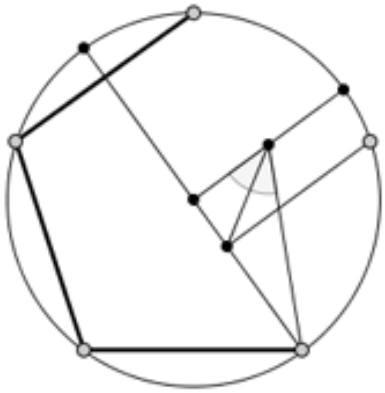
DEFINITION 14.3. Eine Zahl der Form $2^{2^r} + 1$, wobei r eine natürliche Zahl ist, heißt *Fermat-Zahl*.

SATZ 14.4. *Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt*

$$n \ = \ 2^\alpha p_1 \cdots p_k$$

hat, wobei die p_i verschiedene Fermatsche Primzahlen sind.

Beweis. Dieser Satz wird in einer Vorlesung über Körpertheorie bzw. Galoistheorie bewiesen. □



Konstruktion eines regulären Fünfecks mit Zirkel und Lineal

Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt. Es ist noch nicht mal bekannt, ob es außer den ersten fünf Fermat-Zahlen

$$3, 5, 17, 257, 65537$$

überhaupt weitere Fermat-Zahlen gibt, die prim sind. Der folgende Satz hilft bei der Auffindung von Primteilern, da er die Suche wesentlich einschränkt.

Satz 14.5. *Sei $F_r = 2^{2^r} + 1$ eine Fermat-Zahl mit $r \geq 2$. Dann erfüllt jeder Primfaktor p von F_r die Bedingung*

$$p = 2^{r+2}a + 1$$

mit einem $a \in \mathbb{N}_+$.

Beweis. Sei also p ein Primteiler von $F_r = 2^{2^r} + 1$. Dies bedeutet, dass in $\mathbb{Z}/(p)$ die Gleichung

$$2^{2^r} = -1$$

vorliegt. Nach quadrieren ist $2^{2^{r+1}} = 1$ und die Ordnung von 2 ist 2^{r+1} (eine kleinere Ordnung ist nicht möglich, da diese ein Teiler von 2^{r+1} sein muss, aber $2^{2^r} \neq 1$ ist). Diese Ordnung ist ein Teiler von $p - 1$, woraus folgt, dass $p = 1 \mod 8$ ist. Dies bedeutet nach dem zweiten Ergänzungssatz zum quadratischen Reziprozitätsgesetz, dass 2 ein Quadratrest modulo p ist. Sei $x^2 = 2 \mod p$. Dann ist aber die Ordnung von x genau 2^{r+2}. Nach dem Schluss von eben ist 2^{r+2} ein Teiler von $p - 1$, was $p = 2^{r+2}a + 1$ bedeutet. □

Satz 14.6. *Zwei verschiedene Fermatsche Zahlen F_m und F_n sind teilerfremd.*

Beweis. Sei $m > n$. Dann ist

$$F_m - 2 = 2^{2^m} - 1 = \left(2^{2^n}\right)^{2^{m-n}} - 1.$$

Hierbei ist 2^{m-n} gerade, und daher ist $F_n = 2^{2^n} + 1$ ein Teiler von dieser Zahl. Das bedeutet, dass ein gemeinsamer Teiler von F_m und von F_n auch ein

Teiler von $F_m - 2$ ist, also ein Teiler von 2. Da alle Fermat-Zahlen ungerade sind, bleibt nur 1 als gemeinsamer Teiler übrig. □

BEMERKUNG 14.7. Aus Satz 14.6 folgt erneut, dass es unendlich viele Primzahlen gibt. Jede Fermatzahl $F_r = 2^{2^r} + 1$ hat mindestens einen Primfaktor p_r, und diese sind alle verschieden.

Sophie Germain Primzahlen

DEFINITION 14.8. Eine Primzahl p mit der Eigenschaft, dass auch $2p + 1$ eine Primzahl ist, heißt *Sophie-Germain-Primzahl*.

Beispiele sind $(2, 5)$, $(3, 7)$, $(5, 11)$, $(11, 23)$, $(23, 47)$, $(29, 59)$, etc. Es ist unbekannt, ob es unendlich viele Sophie Germain Zahlen gibt.

Wir kommen nochmal zurück zu Mersenne-Zahlen und besprechen einige Situation, wo man Aussagen über mögliche Primteiler machen kann.

SATZ 14.9. *Sei p eine Sophie-Germain-Primzahl, $q = 2p + 1$ und M_p die zugehörige Mersenne-Zahl. Dann ist q ein Teiler von M_p genau dann, wenn $q = \pm 1 \mod 8$ ist.*

Beweis. Es ist $q = 2p+1$ ein Teiler von $M_p = 2^p - 1$ genau dann, wenn $2^p = 1$ in $\mathbb{Z}/(q)$ ist. Wegen $p = \frac{q-1}{2}$ ist dies nach dem Euler-Kriterium genau dann der Fall, wenn 2 ein Quadratrest modulo q ist. Dies ist nach dem zweiten Ergänzungssatz genau bei $q = \pm 1 \mod 8$ der Fall. □

BEMERKUNG 14.10. Ist p eine Sophie-Germain Primzahl, die modulo 4 den Rest 3 hat, so ist $q = 2p + 1 = -1 \mod 8$ und nach Satz 14.9 ist q ein Teiler von M_p. Bei $p > 3$ ist dies ein echter Teiler und M_p ist nicht prim.

Für $p = 3$ ist $M_3 = 2^3 - 1 = 7 = 2p + 1$. Für $p = 11$ ist $q = 23$ prim und es ist $23 | M_{11} = 2047$. Für $p = 23$ ist $q = 47$ wieder prim und es folgt, dass M_{23} ein Vielfaches von 47 ist.

Andere notwendige Bedingungen für Primteiler von Mersenne-Zahlen werden im folgenden Satz ausgedrückt.

SATZ 14.11. *Sei p eine ungerade Primzahl und $M_p = 2^p - 1$ die zugehörige Mersenne-Zahl. Ist q ein Primfaktor von M_p, so ist*

$$q = 1 \mod 2p \text{ und } q = \pm 1 \mod 8\,.$$

Beweis. Es sei q ein Teiler von $M_p = 2^p - 1$. Dies bedeutet

$$2^p = 1 \mod q.$$

Dann ist p die Ordnung von 2 in $\mathbb{Z}/(q)$ und nach Lemma 4.6 ist p ein Teiler von $q - 1$. Dies bedeutet wiederum

$$q = 1 \mod p.$$

Da p und q ungerade sind, folgt sogar $q = 1 \mod 2p$. Wenn x ein primitives Element von $\mathbb{Z}/(q)$ ist, so ist $2 = x^{\frac{q-1}{p}j}$, da alle Elemente der Ordnung p sich so schreiben lassen. Da dieser Exponent gerade ist, muss 2 ein Quadratrest sein, und der Satz 7.12 liefert die Kongruenzbedingung modulo 8. □

Pseudo-Primzahlen

Als Pseudo-Primzahlen bezeichnet man grob gesprochen solche Zahlen, die zwar nicht prim sind, aber wesentliche Eigenschaften mit Primzahlen gemeinsam haben.

Definition 14.12. Eine natürliche Zahl n heißt *quasiprim* zur Basis a, wenn $a^{n-1} = 1$ modulo n gilt.

Definition 14.13. Eine natürliche Zahl n, die nicht prim ist, und die die Eigenschaft besitzt, dass für jede zu n teilerfremde ganze Zahl a

$$a^{n-1} \;=\; 1 \mod n$$

gilt, heißt *Carmichael-Zahl*.

Eine Carmichael-Zahl hat also die Eigenschaft, dass sie quasiprim zu jeder zu n teilerfremden Basis a ist.

Satz 14.14. *Eine natürliche nicht-prime Zahl $n \geq 2$ ist genau dann eine Carmichael-Zahl, wenn jeder Primteiler p von n einfach ist und $p-1$ die Zahl $n-1$ teilt.*

Beweis. Sei $n = p_1^{r_1} \cdots p_k^{r_k}$ die kanonische Primfaktorzerlegung. Nach dem chinesischen Restsatz ist

$$(\mathbb{Z}/(n))^\times \;\cong\; (\mathbb{Z}/(p_1^{r_1}))^\times \times \cdots \times (\mathbb{Z}/(p_k^{r_k}))^\times .$$

Sei $a = (a_1, \ldots, a_k)$ eine zu n teilerfremde Zahl und sei vorausgesetzt, dass n eine Carmichael-Zahl ist. Dann ist insbesondere

$$(a_i)^{n-1} \;=\; 1 \mod p_i^{r_i}$$

für jeden Index i. Wählt man für a_i ein primitives Element in $\mathbb{Z}/(p_i^{r_i})$ (was nach Satz 5.11 möglich ist; für $p_i = 2$ ist nichts zu zeigen), so hat dies die Ordnung $(p_i - 1)p_i^{r_i-1}$. Da $n-1$ ein Vielfaches der Ordnung ist und da p_i und $n-1$ teilerfremd sind, folgt, dass $n-1$ ein Vielfaches von $p-1$ ist. Bei $r_i \geq 2$ gibt es Elemente der Ordnung p_i in $(\mathbb{Z}/(p_i^{r_i}))^\times$ (auch bei $p = 2$), und es ergibt sich der Widerspruch $p|(n-1)$. Also sind alle Exponenten einfach.

Für die Umkehrung ist nach Voraussetzung $r_i = 1$. Sei wieder $a = (a_1, \ldots, a_k)$ eine Einheit. Dann ist

$$a^{n-1} \;=\; \left(a_1^{n-1}, \ldots, a_k^{n-1}\right) \;=\; \left(\left(a_1^{p_1-1}\right)^{\frac{n-1}{p_1-1}}, \ldots, \left(a_k^{p_k-1}\right)^{\frac{n-1}{p_k-1}}\right) \;=\; (1, \ldots, 1) \;=\; 1.$$

Also ist n eine Carmichael-Zahl. □

Beispiel 14.15. Die kleinste Carmichael-Zahl ist

$$561 = 3 \cdot 11 \cdot 17.$$

Dies folgt aus Satz 14.14, da 2, 10 und 16 Teiler von 560 sind.

Es ist inzwischen bekannt, dass es unendlich viele Carmichael-Zahlen gibt.

Abbildungsverzeichnis