

**FACHARBEIT**  
im Fach  
**Mathematik**

Thema: **Primzahlen**

**Verfasser:** Susanne Mennecke  
**Leistungskurs:** Mathematik 1  
**Kursleiter:** Herr StD Wilfried Adler

# Inhalt

<b>1. Einleitung</b>	4
<b>2. Definition</b>	5
<b>3. Primfaktorzerlegung von natürlichen Zahlen</b>	6
3.1. Primfaktorzerlegung	6
3.2. Eindeutigkeit der Primfaktorzerlegung	6
<b>4. Anzahl der Primzahlen</b>	8
4.1. Unendlichkeitsbeweis nach Euklid	8
4.2. Unendlichkeitsbeweis nach Euler	9
<b>5. Ermittlung von Primzahlen</b>	11
5.1. Das Sieb des Eratosthenes	11
5.2. Formeln zur Konstruktion von Primzahlen	12
5.2.1. Mersennesche Primzahlen	12
5.2.2. Fermatsche Primzahlen	13
5.2.3. Weitere Formeln zur Konstruktion von Primzahlen	14
5.3. Der kleine Satz von Fermat	14
5.3.1. Vorüberlegungen	14
5.3.2. Herleitung	16
5.4. Der Satz von Wilson	17
5.4.1. Vorüberlegungen	17
5.4.2. Herleitung	18
<b>6. Verteilung von Primzahlen</b>	20
6.1. Allgemeines	20
6.2. Primzahlsatz	20
6.3. Die grafische Darstellung der Primzahlverteilung	23
<b>7. Primzahlen in arithmetischen Folgen</b>	24
<b>8. Die Goldbachsche Vermutung</b>	26
<b>9. Anwendung von Primzahlen in der Kryptographie</b>	29
<b>10. Anhang</b>	31
10.1. Summenregel für unendliche geometrische Reihen	31
10.2. Rechnung 1	31
10.3. Rechnung 2	31
10.4. Tabelle der bekannten Mersenneschen Primzahlen	32
10.5. Der Satz von Euler	33
10.6. Grafische Darstellung aller ungeraden Primzahlen bis 65536	33

<b>11. Literaturverzeichnis</b>	34
11.1. Bücher	34
11.2. Internetadressen	34
11.2.1. Allgemeines	34
11.2.2. Biographien	35
<b>12. Selbstständigkeitserklärung</b>	37

# 1. Einleitung

„Die Mathematik ist die Königin der Wissenschaften, und die Zahlentheorie ist die Königin der Mathematik.“ (Carl Friedrich Gauß; Nr. 3, S. 17<sup>1</sup>)

Die Zahlentheorie hat die Mathematiker schon seit jeher fasziniert. Dies gilt besonders für die Theorie der Primzahlen, einem Teilgebiet der Zahlentheorie. Aber was macht ihre Faszination aus? Primzahlen sind sehr einfach definiert und bieten eine ideale Grundlage für zahlreiche mathematische Sätze und weitere Überlegungen. Sie führen zu den kompliziertesten und verblüffendsten Zusammenhängen, so dass es bis heute noch zahlreiche ungelöste Probleme und offene Fragen um die Primzahlen gibt. Besonders interessant an der Theorie der Primzahlen ist auch, dass es sich hierbei um ein anwendungsorientiertes Gebiet der Mathematik handelt.

Die treffendsten und fesselndsten Worte hat meiner Meinung nach der Mathematiker Don Zagier über die Primzahlen gefunden. Er hat seine Begeisterung folgendermaßen ausgedrückt:

„Es gibt zwei Tatsachen über die Verteilung von Primzahlen[...]. Die eine ist, daß die Primzahlen, trotz ihrer einfachen Definition und Rolle als Bausteine der natürlichen Zahlen, zu den willkürlichsten, widerspenstigsten Objekten gehören, die der Mathematiker überhaupt studiert. Sie wachsen wie Unkraut unter den natürlichen Zahlen, scheinbar keinem anderen Gesetz als dem Zufall unterworfen, und kein Mensch kann voraussagen, wo wieder eine sprießen wird, noch einer Zahl ansehen, ob sie prim ist oder nicht. Die andere Tatsache ist viel verblüffender, denn sie sagt just das Gegenteil – daß die Primzahlen die ungeheuerste Regelmäßigkeit aufzeigen, dass sie durchaus Gesetzen unterworfen sind und diesen mit fast peinlicher Genauigkeit gehorchen.“(Nr. 4, S. 41f.)

---

<sup>1</sup> Im Folgenden habe ich für alle Quellenangaben eine abgekürzte Form verwendet. Die vollständigen Angaben sind nummeriert im Literaturverzeichnis zu finden. Die Zahlen im Text weisen auf die jeweilige Quelle in der Bibliographie hin.  
In diesem Fall Nr. 3: Richard Courant, Herbert Robbins: Was ist Mathematik?

## 2. Definition<sup>2</sup>

Unter einer Primzahl versteht man eine natürliche Zahl  $> 1$ , die nur durch sich selbst und 1 teilbar ist.

Die Zahl 1 ist selbst keine Primzahl, da jede Zahl den Teiler 1 in beliebig hoher Potenz enthält und es sich somit als zweckmäßig erwiesen hat, sie nicht zu den Primzahlen zu zählen.

Dementsprechend ist die 2 die kleinste Primzahl. Sie ist auch die einzige gerade Primzahl, da jede größere gerade Zahl den Faktor 2 enthält.

### Die ersten 100 Primzahlen lauten:

2	3	5	7	11	13	17	19	23	29	31	37	41
43	47	53	59	61	67	71	73	79	83	89	97	101
103	107	109	113	127	131	137	139	149	151	157	163	167
173	179	181	191	193	197	199	211	223	227	229	233	239
241	251	257	263	269	271	277	281	283	293	307	311	313
317	331	337	347	349	353	359	367	373	379	383	389	397
401	409	419	421	431	433	439	443	449	457	461	463	467
479	487	491	499	503	509	521	523	541				

---

<sup>2</sup> nach Nr. 1, S. 7

### 3. Primfaktorzerlegung von natürlichen Zahlen

Die meisten natürlichen Zahlen können in kleinere Faktoren zerlegt werden: z.B.:  $10 = 5 \cdot 2$ ;  $144 = 12 \cdot 3 \cdot 2 \cdot 2$  usw. Primzahlen hingegen lassen sich nicht weiter in ein Produkt aus kleineren Zahlen aufspalten.

Der Fundamentalsatz der elementaren Zahlentheorie besagt, dass Primzahlen die Bausteine für den multiplikativen Aufbau der natürlichen Zahlen sind, also dass jede natürliche Zahl  $n > 1$ , abgesehen von der Reihenfolge der Faktoren, eindeutig als Produkt von Primzahlen darstellbar ist:  $n = p_1 p_2 \cdots p_r$  ( $r=1; r \in \mathbb{N}$ ). Dies möchte ich im Folgenden durch ein indirektes Beweisverfahren zeigen:

#### 3.1. Primfaktorzerlegung<sup>3</sup>

Gegeben sei eine beliebige natürliche Zahl  $n > 1$ , die aber keine Primzahl sein soll.

Wir spalten zunächst den kleinsten Teiler  $p_1 > 1$  ab, der somit Primzahl ist. (Wäre  $p_1$  keine Primzahl, so könnte man  $p_1$  in der Form  $p_1 = a \cdot b$  darstellen, wobei  $a < p_1$  und  $b < p_1$  ist. Die Zahl  $n$  ließe sich somit als  $n = p_1 \cdot q = a \cdot b \cdot q$  darstellen, was der Forderung widerspricht, dass  $p_1$  der kleinste Teiler von  $n$  sein soll.)

Im komplementären Teiler lässt sich nun wieder eine kleinste Primzahl  $p_2 = p_1$  abspalten usw. Da die komplementären Teiler ständig abnehmen, bricht das Verfahren mit einer Primzahl  $p_r$  ab. Auf diese Weise erhalten wir die sogenannte *kanonische Zerlegung* von  $n > 1$ :

$$n = p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_k^{\epsilon_k} \quad (p_1 < p_2 < \dots < p_k), \quad \epsilon_1 = 1; \quad \epsilon_i \in \mathbb{N}$$

#### 3.2. Eindeutigkeit der Primfaktorzerlegung<sup>4</sup>

Nun stellt sich die Frage, ob diese kanonische Zerlegung von  $n$  auch eindeutig ist, oder ob man  $n$  auf mehrere Weisen in Primzahlen zerlegen kann.

Ist dies der Fall, so gibt es eine kleinste natürliche Zahl  $m$  mit der doppelten Zerlegung

<sup>3</sup> nach Nr. 1, S. 7 f.

<sup>4</sup> nach Nr. 2, 20 f.

$$m = p_1 \cdot l \quad (1)$$

$$m = q_1 \cdot u, \quad (2)$$

wobei  $p_1$  und  $q_1$  Primzahlen und  $l$  und  $u$  natürliche Zahlen sind.

Da  $l < m$ , hat  $l$  die eindeutige Primzahlzerlegung

$$l = p_2 p_3 \cdots p_r, \quad (3)$$

ebenso

$$u = q_2 q_3 \cdots q_s. \quad (4)$$

Jedes  $p_i$  ist von jedem  $q_k$  verschieden, (5)

denn wäre  $p_i = q_k$ , dann hätte zum Beispiel  $\frac{m}{p_i} < m$  zwei verschiedene Zer-

legungen, was der Forderung widerspricht, dass  $m$  die kleinste Zahl mit einer doppelten Zerlegung sein soll.

Wir nehmen nun an, dass  $p_1$  die kleinste in den Zerlegungen von  $m$  auftretende Primzahl ist.

Wir bilden die natürliche Zahl  $m' = m - p_1 u$ .

Einerseits ist laut (1)  $m = p_1 l$ , also

$$m' = p_1 l - p_1 u = p_1 (l - u), \quad (6)$$

andererseits gilt laut (2)  $m = q_1 u$ , also

$$m' = q_1 u - p_1 u = (q_1 - p_1) u. \quad (7)$$

$m'$  ist wegen  $m' < m$  eine natürliche Zahl mit eindeutiger Primfaktorzerlegung, ebenso wie die Faktoren  $p_1$ ,  $l - u$ ,  $u$  und  $q_1 - p_1$ .

Wegen (6) kommt in der Zerlegung von  $m'$  der Primfaktor  $p_1$  vor. Folglich muss  $p_1$  auch in (7) als Faktor auftreten.

Laut (4) und (5) ist  $p_1$  kein Teiler von  $u$ , also muss  $p_1$  in der Zerlegung von  $q_1 - p_1$  vorkommen.

Somit ist  $q_1 - p_1 = p_1 h$  ( $h \in \mathbb{N}$ ), d. h. durch Umstellen:  $q_1 = p_1 (h + 1)$ .

Also wäre  $q_1$  eine zusammengesetzte Zahl, was im Widerspruch dazu steht, dass  $q_1$  eine Primzahl sein soll.

Der hier aufgeführte Widerspruch beweist, dass jede natürliche Zahl  $n$  eindeutig in ein Produkt aus Primzahlen zerlegbar ist.

## 4. Anzahl der Primzahlen

Eine der ersten Fragen in der Theorie der Primzahlen ist, ob es von ihnen nur eine endliche Anzahl gibt, oder ob die Menge der Primzahlen unendlich viele Elemente enthält.

Auffallend ist, dass sie immer seltener werden, je weiter man am Zahlenstrahl fortschreitet. Zwischen 1 und 1000 gibt es noch 168 Primzahlen, 135 zwischen 1000 und 2000, 127 zwischen 2000 und 3000 und zwischen 3000 und 4000 findet man nur noch 120 von ihnen. Darüber hinaus gibt es unter den natürlichen Zahlen beliebig lange (aber endliche) Folgen aufeinanderfolgender natürlicher Zahlen, in denen keine einzige Primzahl vorkommt. Dennoch gibt es unendlich viele Primzahlen.

### 4.1. Unendlichkeitsbeweis nach Euklid<sup>5</sup>

Der folgende Beweis geht auf den griechischen Mathematiker *Euklid von Alexandria* (ca. 330 – 275 v. Chr.) zurück, der in seinem Lehrbuch „*Elemente*“ erstmals die Mathematik als strenge Wissenschaft behandelte. Euklid zeigte die Unendlichkeit der Primzahlen durch das indirekte Beweisverfahren.

Wir nehmen an, es gäbe eine letzte, eine größte Primzahl  $q$ . Nun bilden wir das Produkt aller Primzahlen  $p = q$  und addieren 1:

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot (q-1) \cdot q + 1.$$

$n$  ist größer als jede der Primzahlen und muss somit zerlegbar in ein Produkt aus Primzahlen sein. Dividiert man  $n$  nun aber einzeln durch jede der Primzahlen  $p = q$ , so bleibt immer der Rest 1. Daher hat  $n$  keine der Primzahlen als Teiler.

$n$  muss also ein Produkt aus Primzahlen, die größer als  $q$  sind, oder selbst Primzahl sein. Dies ist ein Widerspruch zur Annahme, dass  $q$  die größte vorhandene Primzahl ist.

---

<sup>5</sup> nach Nr. 1, S. 9; Nr. 2, S. 28 f.; Nr. 3, S. 18

## 4.2. Unendlichkeitsbeweis nach Euler<sup>6</sup>

Auch *Leonhard Euler*<sup>7</sup> befasste sich mit dem Unendlichkeitsbeweis von Primzahlen. Wie auch schon Euklid, ging er davon aus, dass die Menge der Primzahlen endlich sei und brachte dies zum Widerspruch.

Die endliche Menge von Primzahlen wird mit  $p_1, p_2, \dots, p_r$  bezeichnet. Jede natürliche Zahl  $n$  lässt sich somit folgendermaßen darstellen:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \quad (k = 0; k \in \mathbb{N}).$$

Nun betrachten wir die Summe der Kehrrüche aller natürlichen Zahlen  $n$ , dargestellt durch ihre Primfaktorzerlegung.

Gäbe es unter den natürlichen Zahlen überhaupt nur eine Primzahl, also wäre  $r = 1$ , so hätte die Summe laut Summenregel für unendliche geometrische Reihen<sup>8</sup> folgende Form:

$$\sum_{k=0}^{\infty} \frac{1}{n} = \sum_{k=0}^{\infty} \frac{1}{p_1^k} = \frac{1}{1 - \frac{1}{p_1}}$$

Wäre  $r = 2$ , dann hätten wir die folgende Reihe:

$$\begin{aligned} \sum_{k_1, k_2 \geq 0} \frac{1}{n} &= \sum_{k_1, k_2 \geq 0} \frac{1}{p_1^{k_1} \cdot p_2^{k_2}} = \\ &= 1 + \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_1^2} + \frac{1}{p_1 \cdot p_2} + \frac{1}{p_2^2} + \frac{1}{p_1^3} + \frac{1}{p_1^2 \cdot p_2} + \frac{1}{p_1 \cdot p_2^2} + \frac{1}{p_2^3} + \dots = \\ &= 1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \dots + \frac{1}{p_2} + \frac{1}{p_1 \cdot p_2} + \frac{1}{p_1^2 \cdot p_2} + \frac{1}{p_1^3 \cdot p_2} + \dots + \\ &+ \frac{1}{p_2^2} + \frac{1}{p_1 \cdot p_2^2} + \frac{1}{p_1^2 \cdot p_2^2} + \frac{1}{p_1^3 \cdot p_2^2} + \dots + \frac{1}{p_2^3} + \dots = \\ &= \left( 1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \dots \right) \left( 1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \frac{1}{p_2^3} + \dots \right) = \end{aligned}$$

<sup>6</sup> nach Nr. 7

<sup>7</sup> \* 1707 Basel, † 1783 Petersburg

Euler studierte neben Mathematik auch Theologie, Medizin und orientalische Sprachen. Er veröffentlichte Arbeiten über reine und angewandte Mathematik, Astronomie, Physik, Analysis des Unendlichen, die Variations- und Differenzrechnung sowie die analytische Zahlentheorie und Differentialgeometrie. Er erblindete 1767.

<sup>8</sup> siehe Anhang 10.1.

$$= \sum_{k_1 \geq 0} \frac{1}{p_1^{k_1}} \cdot \sum_{k_2 \geq 0} \frac{1}{p_2^{k_2}} = \frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}}$$

Dies gilt auch für den allgemeinen Fall ( $r > 2$ ), wie man durch ähnliche Überlegungen zeigen kann:

$$\sum_{k_1, \dots, k_r \geq 0} \frac{1}{n} = \sum_{k_1, \dots, k_r \geq 0} \frac{1}{p_1^{k_1} \cdots p_r^{k_r}} = \sum_{k_1 \geq 0} \frac{1}{p_1^{k_1}} \cdots \sum_{k_r \geq 0} \frac{1}{p_r^{k_r}} = \frac{1}{1 - \frac{1}{p_1}} \cdots \frac{1}{1 - \frac{1}{p_r}}$$

also:

$$\sum_{n \geq 1} \frac{1}{n} = \prod_{i=1}^r \frac{1}{1 - \frac{1}{p_i}}$$

Die harmonische Reihe auf der linken Seite der Gleichung divergiert. Rechts dagegen steht ein endlicher Wert (weil  $r$  endlich ist). Damit tritt ein Widerspruch auf, der unsere Annahme von der endlichen Primzahlenanzahl widerlegt.

## 5. Ermittlung von Primzahlen

Wir wissen nun, dass es unendlich viele Primzahlen gibt. Aber wie kann man am schnellsten eine Primzahltafel, d.h. eine Liste aller Primzahlen bis zu einer bestimmten Zahl, aufstellen? Denn jede einzelne Zahl auf ihre Zerlegbarkeit in kleinere Faktoren zu prüfen, wird schnell sehr mühsam.

### 5.1. Das Sieb des Eratosthenes<sup>9</sup>

Das einfachste Verfahren, um alle Primzahlen unter einer gegebenen Zahl  $n$  ausfindig zu machen, ist das „Sieb des Eratosthenes“. Benannt ist es nach seinem Erfinder, dem kyrenischen Mathematiker, Geographen und Dichter *Eratosthenes*<sup>10</sup>.

Um nach diesem Verfahren alle Primzahlen unterhalb einer gegebenen Zahl  $n$  anzugeben, schreibt man sich alle Zahlen von 2 bis  $n$  auf.

z.B.: 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27

Nun streicht man alle echten Vielfachen von 2. Die Zahl 2 selbst bleibt als Primzahl stehen.

2 3 4 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~ 27

Die erste nicht gestrichene Zahl ist die Primzahl 3; alle Vielfachen von 3 werden wieder gestrichen.

2 3 4 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ 16 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ 25 ~~26~~ 27

Die nächste nicht gestrichene Zahl ist die Primzahl 5; man streicht abermals alle Vielfachen von 5.

2 3 4 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ 27

<sup>9</sup> nach Nr. 1, S. 9 f.; Nr. 3, S. 23 – 25

<sup>10</sup> ca. 275 – 194 v. Chr.

Eratosthenes war Leiter der Bibliothek in Alexandria, wo er seinen Studien nachging. Er fertigte u.a. als Erster eine umfassende kartographische Aufnahme der zur seiner Zeit bekannten Erde an. Zu diesem Zweck überzog er sie mit einem Gradnetz und bestimmte (unter Annahme der Kugelform!) ihren Umfang. Die Ergebnisse veröffentlichte er in seinem Werk *Geographika*.

So fährt man bis zur ersten Primzahl  $p$  fort, für die gilt  $p > \sqrt{n}$ . Alle nun noch nicht durchgestrichenen Zahlen sind Primzahlen, denn die Vielfachen  $k \cdot p = n$  wurden wegen  $k = \sqrt{n}$  schon früher als Vielfache von  $k$  gestrichen. Man hat also alle Primzahlen unterhalb von  $n$  gefunden.

## 5.2. Formeln zur Konstruktion von Primzahlen

In der Geschichte der Primzahltheorie hat man oft versucht, einfache arithmetische Formeln zu finden, die als Wertemenge lauter Primzahlen haben. Noch hat man keine Funktion gefunden, die nur Primzahlen liefert. Jedoch wurde erkannt, dass manche Primzahlen von einer ganz bestimmten Form sind.

### 5.2.1. Mersennesche Primzahlen<sup>11</sup>

Diese Primzahlen werden nach dem französischen Mönch *Marin Mersenne*<sup>12</sup> benannt.

Sie haben die Form  $M(n) = 2^n - 1$ , wobei  $n$  selbst auch eine Primzahl sein muss.

Denn falls  $n$  sich in Faktoren  $k \cdot m$  zerlegen lässt, so kann man auch

$$M(n = km) = 2^{km} - 1 = (2^m - 1)(2^{(k-1)m} + 2^{(k-2)m} + \dots + 2^m + 1)$$

in Faktoren zerlegen<sup>13</sup>.

Bis heute (Feb. 2003) hat man 39 solche Mersenneschen Primzahlen gefunden<sup>14</sup>. Die zur Zeit größte bekannte Primzahl ist die Mersennsche Zahl  $2^{13466917} - 1$  mit über 4 Millionen Dezimalstellen. Sie wurde am 14.11.2001 im Rahmen des *GIMPS-Projekt* vom Kanadier *Michael Cameron* gefunden. Das **Great- Internet- Mersenne- Prime- Search-** Projekt wurde 1996 von *George Woltman* ins Leben gerufen, um noch größere als die bis dahin bekannten Mersenneschen Primzahlen zu finden. Installiert man das kostenlose Programm auf seinem Computer, kann man dieses Projekt unterstützen und helfen die

<sup>11</sup> nach Nr. 8; Nr. 9

<sup>12</sup> \* 1588 Maine, † 1648 Paris; frz. Theologe, Philosoph, Musik- und Naturwissenschaftler  
Mersenne korrespondierte mit den führenden Köpfen seiner Zeit, wie Descartes, Galilei, Hobbes etc. und pflegte zu einigen auch enge persönliche Beziehungen. In der Physik waren seine Forschungen zur Akustik wegweisend, für die Musikwissenschaft stellen insbesondere seine Veröffentlichungen zur Instrumentenkunde eine Fundgrube dar.

<sup>13</sup> siehe Anhang 10.2.

<sup>14</sup> siehe Anhang 10.4.

umfangreichen Berechnungen durchzuführen, die nötig sind, um eine solch hohe Zahl auf ihre Teiler zu überprüfen. Dies geschieht nebenbei, während man im Internet ist.

Ob es unendlich viele Mersennesche Primzahlen gibt, ist unbekannt.

### 5.2.2. Fermatsche Primzahlen<sup>15</sup>

Hierbei handelt es sich um Zahlen der Form:  $F(n) = 2^n + 1$ , mit  $n = 2^k$ , wobei  $k$  eine natürliche Zahl ist. Sie werden benannt nach dem Franzosen *Pierre de Fermat*<sup>16</sup>.

$n$  muss selbst eine Potenz von 2 sein, denn besäße  $n$  einen ungeraden Faktor  $u > 1$ , so wäre  $F(n)$  keine Primzahl, wie folgende kurze Überlegung zeigt.

Es sei  $n = c \cdot u$ , wobei  $c$  eine beliebige natürliche Zahl und  $u$  eine ungerade natürliche Zahl ist.  $F$  lässt sich somit als  $F = 2^{cu} + 1 = a^u + 1$  mit  $a = 2^c$  darstellen.  $F$  hat nun die folgende Zerlegung:

$$F = a^u + 1 = (a+1)(a^{u-1} - a^{u-2} + \dots + a^2 - a + 1)$$

und ist somit keine Primzahl<sup>17</sup>.

Fermat untersuchte die ersten Zahlen der Form  $F(k) = 2^{2^k} + 1$  und bemerkte, dass sich für  $F(0)$ ,  $F(1)$ ,  $F(2)$ ,  $F(3)$  und  $F(4)$  Primzahlen ergeben:

$$k = 0 \Rightarrow F(0) = 2 + 1 = 3$$

$$k = 1 \Rightarrow F(1) = 2^2 + 1 = 5$$

$$k = 2 \Rightarrow F(2) = 2^{2^2} + 1 = 17$$

$$k = 3 \Rightarrow F(3) = 2^{2^3} + 1 = 257$$

$$k = 4 \Rightarrow F(4) = 2^{2^4} + 1 = 65537$$

Daraufhin äußerte er die Vermutung, dass alle solche Zahlen Primzahlen sind. Erst 100 Jahre später, im Jahre 1732, widerlegte dies Euler. Er fand heraus,

<sup>15</sup> nach Nr.3, S. 21; Nr. 10; Nr. 11

<sup>16</sup> \* 1601 Lomagne, † 1665 Castres

Fermat studierte in Toulouse Rechtswissenschaften und wurde Anwalt. Er betrieb Mathematik eigentlich nur als Hobby, wobei sein Interesse zunächst nur der antiken Mathematik galt. Dennoch lieferte Fermat eine Menge anregender Sätze und Problemstellungen zur Zahlentheorie, wie zum Beispiel den großen und kleinen Satz von Fermat.

<sup>17</sup> siehe auch Anhang 10.3.

dass schon die nächste Zahl  $2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$  keine Primzahl ist.

Bis heute hat man keine weitere Primzahl dieser Form gefunden. Andererseits hat man aber auch noch nicht bewiesen, dass es keine weitere gibt.

### 5.2.3. Weitere Formeln zur Konstruktion von Primzahlen<sup>18</sup>

Ein anderer, einfacher Ausdruck, der viele Primzahlen liefert, ist

$$f(n) = n^2 - n + 41.$$

Wir erhalten für  $n = 1, 2, 3, \dots, 40$  immer neue Primzahlen. Für  $n = 41$  ergibt sich jedoch  $f(n) = 41^2$  und somit keine Primzahl.

Ebenso bildet der Ausdruck  $g(n) = n^2 - 79n + 1601$  Primzahlen für alle  $n$  bis 79. Er versagt aber für  $n = 80$ .

Im Allgemeinen hat es sich als sinnlos erwiesen, nach Ausdrücken zu suchen, die nur, oder sogar sämtliche, Primzahlen ergeben.

## 5.3. Der kleine Satz von Fermat<sup>19</sup>

*Pierre de Fermat* beschäftigte sich sein ganzes Leben lang gerne mit Primzahlen. Sein „kleiner“ Satz über diese, ein Spezialfall des Satzes von Euler<sup>20</sup>, auf den ich hier aber nicht näher eingehen will, hat in der Primzahltheorie große Bedeutung erlangt.

### 5.3.1. Vorüberlegungen

Für die Herleitung des kleinen Satzes von Fermat sind folgende kurze Vorüberlegungen notwendig:

#### 1. Kongruenzen

Zwei ganze Zahlen heißen kongruent modulo  $n$  (in Zeichen  $a \equiv b \pmod{n}$ ), wenn bei der Division der beiden Zahlen  $a$  und  $b$  durch  $n$  der selbe Rest bleibt. Dies ist gleichbedeutend damit, dass  $n$  ein Vielfaches von  $a - b$  ist.

Für Kongruenzen sind die Addition, die Subtraktion und die Multiplikation eindeutig definiert. Für die Division trifft dies nicht immer zu.

---

<sup>18</sup> nach Nr. 2, S. 27; Nr. 3, S. 21

<sup>19</sup> nach Nr. 11; Nr. 12; Nr. 5, S. 72 f.

<sup>20</sup> siehe Anhang 10.5.

Ist  $c$  aber nicht durch  $n$  teilbar, so kann man kürzen, d.h. aus

$$ac \equiv bc \pmod{n}$$

folgt

$$a \equiv b \pmod{n}.$$

Ist  $a$  ein Vielfaches von  $n$ , so gilt:

$$0 \equiv a \pmod{n}$$

## 2. Teilbarkeit der Binomialkoeffizienten

Stellt man die Binomialkoeffizienten mit Hilfe des Pascalschen Dreiecks dar, fällt auf, dass alle Binomialkoeffizienten (bis auf die Einsen am Rand) in einer Zeile durch die Zeilennummer teilbar sind, wenn diese eine Primzahl ist. Dies lässt sich folgendermaßen zeigen:

$$\text{Ist } k < n, \text{ dann gilt: } \binom{n}{k} \cdot k! = \frac{n!}{(n-k)!} = n(n-1) \cdots (n-k+1)$$

Also ist  $\binom{n}{k} \cdot k!$  durch  $n$  teilbar. Wenn  $n$  aber eine Primzahl ist, dann ist  $k!$  wegen  $k < n$  nicht durch  $n$  dividierbar (in dem Produkt  $k!$  kommt die Primzahl  $n$  als Faktor nicht vor, also ist  $k!$  auch nicht durch sie teilbar). Folglich muss  $\binom{n}{k}$  durch  $n$  dividierbar sein, da, wenn ein Produkt zweier Zahlen durch eine Primzahl teilbar ist, mindestens einer der beiden Faktoren durch sie teilbar sein muss.

Somit gilt:

$$\text{Ist } n \in \mathbb{P}, \text{ dann gilt } n \mid \binom{n}{k} \text{ für } k = 1, \dots, n-1. \quad (1)$$

Umgekehrt gilt auch, wenn  $n$  keine Primzahl ist, teilt  $n$  auch nicht  $\binom{n}{k}$ :

Denn ist  $n$  keine Primzahl, so enthält sie einen kleinsten Primfaktor  $p < n$  genau  $k$  mal, das heißt  $n$  ist durch  $p^k$ , aber nicht durch  $p^{k+1}$  teilbar. Somit kann man  $n$  als  $p^k \cdot u$  darstellen. Unter den  $p$  aufeinanderfolgenden Zahlen  $n, n-1, \dots, n-p+1$  ist nur  $n$  durch  $p$  teilbar (das nächste Vielfache von  $p$  wäre erst  $n-p$ ).

Also kürzt sich aus dem Ausdruck

$$\binom{n}{p} = \binom{p^k \cdot u}{p} = \frac{(p^k \cdot u) \cdot (n-1) \cdots (n-p+1)}{1 \cdot 2 \cdots (p-1) \cdot p} = \frac{(p^{k-1} \cdot u) \cdot (n-1) \cdots (n-p+1)}{1 \cdot 2 \cdots (p-1)}$$

ein Faktor  $p$  aus  $n$  heraus.  $\binom{n}{p}$  ist nun nur noch durch  $p^{k-1}$  teilbar und folglich nicht mehr durch  $n$ .

### 5.3.2. Herleitung

Nach dem Binomischen Satz gilt:

$$(a+b)^n = \binom{n}{n} a^n + \binom{n}{n-1} a^{n-1} b + \dots + \binom{n}{1} a b^{n-1} + \binom{n}{0} b^n$$

Es sei nun  $n$  eine Primzahl  $p$ ,  $a = x$  und  $b = 1$

$$(x+1)^p = x^p + \binom{p}{p-1} x^{p-1} + \dots + \binom{p}{1} x + 1$$

Laut (1) sind alle  $\binom{p}{k}$  durch  $p$  teilbar. Folglich gilt:

$$(x+1)^p \equiv x^p + 1 \pmod{p}$$

Wählt man nun  $x = 1$ , so folgt

$$2^p \equiv 2 \pmod{p}$$

Setzt man  $x = 2$ , erhält man

$$3^p \equiv 2^p + 1 \pmod{p}$$

da aber  $2^p \equiv 2 \pmod{p}$ , gilt:

$$3^p \equiv 2^p + 1 \equiv 2 + 1 \equiv 3 \pmod{p}$$

Diese Verfahren kann man für jedes beliebige  $x$  fortsetzen.

Allgemein ergibt sich:

$$n^p \equiv n \pmod{p} \quad p \in ? \quad (2)$$

Sind  $n$  und  $p$  teilerfremd, kann man diese Kongruenz durch  $n$  teilen und man erhält:

$$n^{p-1} \equiv 1 \pmod{p} \quad p \in ?, p \text{ und } n \text{ teilerfremd} \quad (3)$$

Satz (2) und (3) heißen kleiner Fermatscher Satz.

Oder anders ausgedrückt: ist  $p$  eine Primzahl und  $n$  eine natürliche Zahl, die kein Vielfaches von  $p$  ist, dann ist  $n^{p-1}$  stets um 1 größer als das nächstkleinere Vielfache von  $p$ .

Leider gibt es auch zusammengesetzte Zahlen  $C$  (sogenannte *Carmichaelsche Zahlen*), für die gilt:

$$n^{C-1} \equiv 1 \pmod{C}$$

Somit kann der kleine Satz von Fermat zwar nicht direkt als Primzahltest gebraucht werden, er dient aber als Grundlage fast aller wichtiger Testverfahren.

Der kleine Satz von Fermat ist eine notwendige Bedingung für die Primeigenschaft, jedoch nicht hinreichend.

## 5.4. Der Satz von Wilson<sup>21</sup>

Ein weiterer Satz über Primzahlen ist der Satz von Wilson. Er wurde von dem englischen Mathematiker *John Wilson* (1741 – 1793) entdeckt und erstmals 1771 von dem französischen Mathematiker *Joseph-Louis Lagrange*<sup>22</sup> bewiesen.

### 5.4.1. Vorüberlegungen

*Das inverse Element*

Unter dem inversen Element zu einer Zahl  $a$ , versteht man die Zahl  $a^{-1}$ , mit der man  $a$  verknüpfen muss, um das neutrale Element zu erhalten.

Bezüglich der Multiplikation ist das neutrale Element die Zahl 1. Also gilt:

$$a \cdot a^{-1} = 1$$

Bei der Kongruenzrechnung ist das inverse Element bezüglich der Multiplikation folgendermaßen definiert:

$$a \cdot a^{-1} \equiv 1 \pmod{p}$$

Ich möchte nun zeigen, dass es für jedes  $0 < a < p$  einen inversen Partner  $0 < a^{-1} < p$  gibt.

Dazu betrachten wir die Zahlen  $m_1 = 1 \cdot a$ ;  $m_2 = 2 \cdot a$ ; ...;  $m_{p-1} = (p-1) \cdot a$ , wobei  $p$  eine Primzahl und  $0 < a < p$  ist.

<sup>21</sup> nach Nr. 13; Nr. 14; Nr. 19

<sup>22</sup> \* 1736 Turin, † 1813 Paris

Lagranges bedeutendstes Werk ist seine Arbeit zur Analytischen Mechanik. In beinahe der Hälfte seiner Arbeiten befasste er sich mit den Bewegungen der Himmelskörper. Aber im Bereich der Zahlentheorie machte er große Fortschritte und bewies den Satz, dass sich jede ganze Zahl als Summe von höchstens 4 Quadraten darstellen lässt.

Die Zahlen  $m_i$  sind untereinander alle inkongruent.

Denn wäre  $m_k \equiv m_s \pmod{p}$ ,

so folgt

$$ka \equiv sa \pmod{p}$$

also

$$k \equiv s \pmod{p} \quad (\text{da } a \text{ und } p \text{ teilerfremd sind})$$

Da  $k$  und  $s$  aber kleiner als  $p$  sind, gilt dies aber nur, wenn  $k = s$ .

Auch die Reste  $1, 2, 3, \dots, p-1$  sind inkongruent zueinander.

Folglich kann man jeder Zahl  $m_i$  eine Restklasse von 1 bis  $p-1$  zuordnen.

Es ergibt sich für jedes  $0 < y < p$  genau ein  $0 < x < p$ , so dass gilt:

$$m_x \equiv a \cdot x \equiv y \pmod{p} \quad (p \in \mathbb{P}; 0 < a < p)$$

Insbesondere existiert zu jedem  $0 < a < p$  ein  $0 < a^{-1} < p$ , so dass gilt:

$$a \cdot a^{-1} \equiv 1 \pmod{p},$$

also ein eindeutig bestimmtes Inverses. q.e.d.

### 5.4.2. Herleitung

Wir suchen nun alle zu sich selbst inversen Kongruenzen:

Hierbei sei  $p$  eine Primzahl und für  $a$  gelte:  $0 < a < p$ .

Da  $a^{-1} = a$  gelten soll, folgt also:

$$a^2 \equiv 1 \pmod{p}$$

oder anders gesagt:

$$a^2 - 1 = kp \quad (k \in \mathbb{N})$$

$$(a - 1)(a + 1) = kp$$

Das heißt  $p \mid (a - 1)$  oder  $p \mid (a + 1)$ .

Aus  $p \mid (a - 1)$  und  $0 < a < p$  folgt

$$a - 1 = kp, \text{ also } a = kp + 1 \Rightarrow a = 1$$

und aus  $p \mid (a + 1)$  und  $0 < a < p$  folgt

$$a + 1 = kp, \text{ also } a = kp - 1 \Rightarrow a = p - 1$$

Somit sind 1 und  $p-1$  die Selbstinversen der Kongruenzen.

Im Produkt  $(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2) \cdot (p-1) \pmod{p}$  hat nun also jeder der Faktoren, außer der 1 und  $p-1$ , einen inversen Partner.

Also gilt:

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$$

$$(p-1)! \equiv -1 \pmod{p}$$

Diese Gleichung wird als Satz von Wilson bezeichnet.

Dieser sagt aus, dass die natürliche Zahl  $p$  genau dann eine Primzahl ist, wenn sie  $(p-1)! + 1$  teilt.

Ist  $p$  keine Primzahl, also  $p = s \cdot t$  mit  $s, t > 1$ , so enthält  $(p-1)!$  die Faktoren  $s$  und  $t$  und folglich wäre zwar  $(p-1)!$ , aber nicht mehr  $(p-1)! + 1$  durch  $p$  teilbar.

Somit ist der Satz von Wilson, im Gegensatz zum kleinen Satz von Fermat, eine sowohl notwendige, als auch hinreichende Bedingung dafür, dass eine Zahl prim ist und kann direkt als Primzahltest dienen.

Da die Fakultätsfunktion aber sehr schnell ansteigt, lässt der Test sich in der Praxis kaum gebrauchen.

## 6. Verteilung von Primzahlen

### 6.1. Allgemeines<sup>23</sup>

Wie zuvor schon erwähnt, werden die Primzahlen, je weiter man in der Zahlenreihe fortschreitet, immer seltener. So gibt es, wie folgendes Beispiel zeigt, in der Folge der Primzahlen beliebig große Lücken.

Unter den  $m$  aufeinanderfolgenden Zahlen  $(m + 1)! + 2, (m + 1)! + 3, \dots, (m + 1)! + m + 1$  ist keine Primzahl, da die erste durch 2, die zweite durch 3, ... und die letzte durch  $m + 1$  teilbar ist.

Andererseits gibt es aber auch sogenannte *Primzahlzwillinge*. Das sind Primzahlen  $p$  und  $q$  mit dem minimalen Abstand 2, z.B.: 41, 43; 2309, 2311; 10016957, 10016959. Ob es unendlich viele von diesen Zwillingspaaren gibt, oder nur eine endliche Anzahl, ist bis heute noch unbekannt.

Neben den Zwillingen gibt es auch noch *Primzahltrillinge*  $p, p + 2, p + 6$ , bzw.  $p, p + 4, p + 6$  und *Primzahlvierlinge*  $p, p + 2, p + 6, p + 8$ .

Beispiele: 5, 7, 11; 10014491, 10014493, 10014497; 294311, 294313, 294317, 294319; 299471, 299473, 299477, 299479.

### 6.2. Primzahlsatz<sup>24</sup>

Bei der Untersuchung der Primzahlverteilung konzentriert man sich in erster Linie auf die Untersuchung der *Primzahlfunktion*  $\pi(x)$ , welche die Anzahl der Primzahlen bis zur Zahl  $x$  angibt. So ist  $\pi(1) = 0$ ,  $\pi(2) = 1$ ,  $\pi(20) = 8$  und  $\pi(p_n) = n$ , wenn  $p_n$  die  $n$ -te Primzahl ist.

Obwohl noch keine einfache Formel für  $\pi(x)$  bekannt ist, lassen sich doch Aussagen über ihre Größenordnung machen. So zum Beispiel im Primzahlsatz, der schon von *Carl Friedrich Gauß*<sup>25</sup> vermutet und erstmals von *Jacques*

<sup>23</sup> nach Nr. 1, S. 10 f.

<sup>24</sup> nach Nr. 1, S. 11; Nr. 3, S. 24; Nr. 4, S. 48 – 50

<sup>25</sup> \* 1777 Braunschweig, † 1855 Göttingen.

Gauß war ein hochbegabter Mathematiker, Astronom und Physiker. Er veröffentlichte grundlegende Werke über die höhere Arithmetik, Differentialgeometrie und die Bewegung der Himmelskörper. Astronomisches Hauptwerk: Theorie der Bewegung der Himmelskörper.

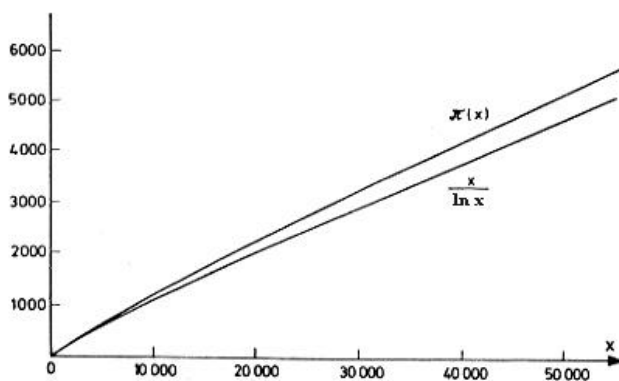
Salomon Hadamard<sup>26</sup> und Charles Jean Gustave Nicolas Baron de la Vallée Poussin<sup>27</sup> bewiesen wurde. Er besagt, dass das Verhältnis von  $\pi(x)$  und der Funktion  $f(x) = \frac{x}{\ln x}$  mit wachsendem  $x$  gegen 1 strebt und man somit, für große  $x$ ,  $\pi(x)$  mit  $f(x)$  gleichsetzen kann, da der relative Fehler  $\frac{\pi(x) - f(x)}{\pi(x)}$  verschwindend klein wird.

**Primzahlsatz:**  $\lim_{x \rightarrow \infty} \frac{\pi(x) \ln x}{x} = 1$  oder  $\pi(x) \sim \frac{x}{\ln x}$   
 (~ heißt asymptotisch gleich)

Bemerkenswert an der Erkenntnis, dass das Verhalten der Primzahlfunktion mit Hilfe der Logarithmusfunktion beschrieben werden kann, ist, dass zwei so verschiedene mathematische Begriffe wie  $\pi(x)$  und  $\ln x$ , die scheinbar gar nichts miteinander zu tun haben, doch so eng miteinander verknüpft sind.

Wenn man aber den Graph der Funktion  $\frac{x}{\ln x}$  mit  $\pi(x)$  vergleicht, sieht man,

dass die Funktion  $\frac{x}{\ln x}$  das Verhalten von  $\pi(x)$  zwar qualitativ wiedergibt, ein echter Fehler aber immer noch bestehen bleibt.



Folglich hat man versucht, bessere Näherungen für  $\pi(x)$  zu finden.

<sup>26</sup> \* 1865 Versailles, † 1963 Paris

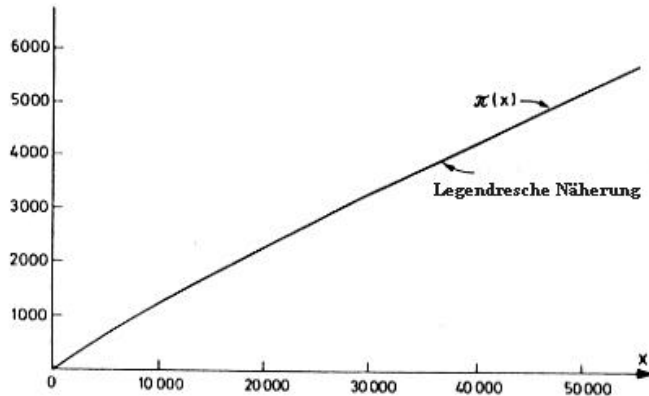
Hadamard gilt als der Schöpfer des Prinzips der topologischen Dualität. Andere Beiträge Hadamard's befassten sich mit der Theorie von Integralfunktionen, Extremwerten von Funktionen und partiellen Differentialgleichungen der mathematischen Physik.

<sup>27</sup> \* 1866 Louvain, † 1962 Louvain (Belgien)

De la Vallée Poussin studierte Ingenieurwesen und anschließend Mathematik. Mit 26 wurde er, als Nachfolger von Louis-Philippe Gilbert, an die Universität von Louvain berufen. Er veröffentlichte verschiedenen Arbeiten auf dem Gebiet der Analysis und vor allem der Zahlentheorie. De la Vallée Poussin beschäftigte sich eingehend mit der Riemanschen Zetafunktion.

So entdeckte *Adrien- Marie Legendre*<sup>28</sup> 1808, dass man eine besonders gute Näherung enthält, wenn man noch die Zahl 1,08366 vom Logarithmus abzieht:

$$\pi(x) \sim \frac{x}{\ln x - 1,08366}$$



Andere, noch bessere Approximationen zu  $\pi(x)$  entwickelten Gauß (logarithmische Summe, bzw. logarithmisches Integral) und *Bernhard Riemann*<sup>29</sup>.

Obwohl man die Formulierung des Primzahlsatzes leicht verstehen kann, ist sein Beweis äußerst kompliziert und im Rahmen dieser Arbeit und ohne die Kenntnis der höheren Mathematik nicht durchführbar.

<sup>28</sup> \* 1752, † 1833

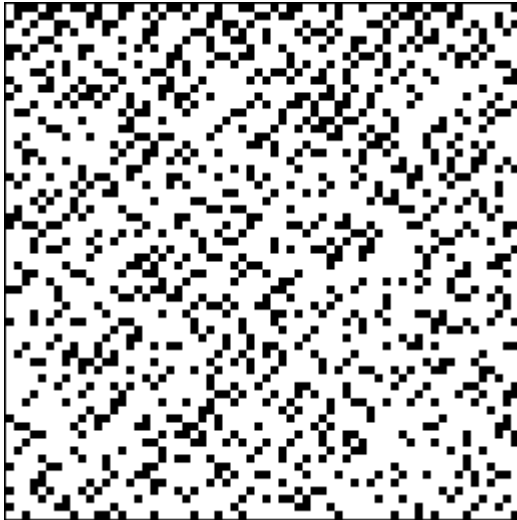
Legendre veröffentlichte auf vielen Gebieten Arbeiten, so zum Beispiel über die Planetenbahnen, auf dem Gebiet der Zahlentheorie und der Theorie der elliptischen Funktionen. Er war gut befreundet mit Laplace und Lagrange - mit Gauß geriet er aber immer wieder aneinander. Sein Lebensende verbrachte er in Armut in Paris.

<sup>29</sup> \* 1826 bei Hannover, † 1866

Riemann war sehr früh von den Primzahlen und ihren Eigenschaften fasziniert. Zum Beispiel beschäftigte er sich mit dem Problem, eine Formel zu finden, nach der man die Anzahl der Primzahlen bis zu einer gewissen Zahl  $n$  berechnen kann. Ab 1853 beschäftigte er sich mit dem Studium der mathematischen Physik. Sein Vortrag „über die Hypothesen, die der Geometrie zu Grunde liegen“ wurde ein Meisterwerk der Mathematik.

### 6.3. Die grafische Darstellung der Primzahlverteilung<sup>30</sup>

Prof. Dr. Otto Forster vom mathematischen Institut der Ludwig- Maximilian- Universität München beschäftigt sich mit der grafischen Darstellung der Primzahlverteilung.



Diese Bild zeigt die Verteilung aller ungeraden Primzahlen kleiner als 8192. Es ist in 64 Zeilen und 64 Spalten mit insgesamt 4096 schwarzen und weißen Quadraten unterteilt. Diese Quadrate sind reihenweise von 0 bis 4095 nummeriert, wobei das  $n$ - te Quadrat schwarz ist, wenn die Zahl  $2n + 1$  eine Primzahl darstellt.

So steht zum Beispiel das schwarze Quadrat in der rechten oberen Ecke für die Primzahl 127, das schwarze Quadrat in der rechten unteren Ecke stellt die Primzahl 8191 dar.

Sehr schön erkennbar sind in dieser Grafik Primzahlzwillinge. Sie sind als zwei aufeinanderfolgende Quadrate  $||$  gekennzeichnet. Die Folgen  $||?|$  bzw.  $|?||$  zeigen Primzahldrillinge und  $||?||$  die noch selteneren Primzahlvierlinge.

Ebenfalls sehr gut ersichtlich ist die Unregelmäßigkeit der Primzahlverteilung und dass die Primzahldichte mit fortschreitenden Zahlen immer mehr abnimmt.<sup>31</sup>

<sup>30</sup> nach Nr. 15

<sup>31</sup> siehe auch Anhang 10.6.

## 7. Primzahlen in arithmetischen Folgen<sup>32</sup>

Satz von *Johann Peter Gustav Lejeune Dirichlet*<sup>33</sup>:

Jede arithmetische Folge  $a, a + d, a + 2d, \dots$ ;  $d > 0$ , wobei  $a$  und  $d$  keinen gemeinsamen Teiler  $> 1$  haben, enthält unendlich viele Primzahlen.

Da der allgemeine Beweis dieses Satzes nicht ohne die höhere Infinitesimalrechnung und Funktionstheorie auskommt, möchte ich mich hier mit dem Beweis von 2 Spezialfällen begnügen:

Alle ungeraden Primzahlen haben die Form  $4n + 1$  oder  $4n + 3$ .

Mit dem Euklidischen Beweisverfahren kann man leicht zeigen, dass zum Beispiel  $4n + 3$  unendlich viele Primzahlen  $p$  enthält:

Wir nehmen an, es gäbe nur eine endliche Anzahl an Primzahlen der Form  $4n + 3$ . Nun bilden wir die Zahl

$$P = 2^2 \cdot 3 \cdot 5 \cdot \dots \cdot (p-1) \cdot p - 1,$$

in der alle Primzahlen  $= p$  als Faktoren im Minuend vorkommen.  $p$  soll die größte Primzahl der Form  $4n + 3$  sein.

$P$  hat die Form  $4n + 3$ :

$$P = 2^2 \cdot 3 \cdot 5 \cdot \dots \cdot p - 1 = 2^2 \cdot 3 \cdot 5 \cdot \dots \cdot p - 1 + 3 - 3 = 4(3 \cdot 5 \cdot \dots \cdot p - 1) + 3$$

$P$  kann nicht das Produkt von ausschließlich Primzahlen der Form  $4n + 1$  sein, da ein solches Produkt auch immer die Form  $4n + 1$  hat:

$$(4a + 1)(4b + 1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1.$$

Somit ist  $P$  durch eine Primzahl von der Form  $4n + 3$  teilbar, die größer als  $p$  ist, was im Widerspruch zur Annahme steht, dass  $p$  die größte Primzahl der Form  $4n + 3$  ist. Es muss also unendlich viele Primzahlen der Form  $4n + 3$  geben.

Ganz ähnlich erfolgt der Beweis, dass es unendlich viele Primzahlen von der Form  $6n + 5$  gibt.

Außer 2 und 3 hat jede Primzahl die Form  $6n + 1$  oder  $6n + 5$ .

<sup>32</sup> nach Nr. 1, S. 11f.; Nr. 3, S. 21f.

<sup>33</sup> \* 1805 Düren, † 1859 Göttingen

Lejeune Dirichlet war Hauslehrer in Paris. Nach dem Tod von Gauß wurde er an die Universität von Göttingen berufen. Er nahm Einfluss auf Einstein, Dedekind und Riemann. Dirichlet veröffentlichte Arbeiten auf dem Gebiet der Zahlentheorie und der Analysis.

$$P = 2 \cdot 3 \cdot \dots \cdot p - 1 = 6(7 \cdot 11 \cdot \dots \cdot p - 1) + 5$$

hat wieder die Form  $6n + 5$ .

$P$  kann nicht nur aus Faktoren der Form  $6n + 1$  bestehen, da ein solches Produkt wieder die Form  $6n + 1$  hat (analog dem Produkt von  $4n + 1$ ).

Folglich muss es für jedes  $p$  eine Primzahl der Form  $6n + 5$  geben, die größer als  $p$  ist.

## 8. Die Goldbachsche Vermutung<sup>34</sup>

1742 stellte *Christian Goldbach*<sup>35</sup>, ein Lehrer des russischen Zaren Peter II in einem Brief an *Euler* folgende zwei Vermutungen auf:

- 1) Jede gerade Zahl  $> 2$  lässt sich als Summe von zwei Primzahlen darstellen.
  - 2) Jede natürliche Zahl  $> 5$  lässt sich als Summe von drei Primzahlen darstellen.
- Er bat Euler, er möge ihm diese beiden Vermutungen beweisen, aber Euler gelang dies trotz jahrelanger Bemühungen nicht.

Offenbar kann man 2) aus 1) folgern, da, wenn man jede gerade natürliche Zahl  $> 2$  als Summe von 2 Primzahlen darstellen kann, durch Addition der Primzahl 3 immer eine neue ungerade natürliche Zahl entsteht und somit alle natürlichen Zahlen  $> 5$  bildbar sind.

Der leichtere Beweis, dass sich jede natürliche Zahl  $n > 6$  als Summe ungleicher Primzahlen darstellen lässt (also ohne Einschränkung der Anzahl der Summanden), ist folgendermaßen zu vollführen:

Die Zerlegungen der 13 Zahlen:

$$\begin{aligned} Z_0 = \{ & 7 = 7; 8 = 5 + 3; 9 = 7 + 2; 10 = 7 + 3; 11 = 11; 12 = 7 + 5; 13 = 11 + 2; \\ & 14 = 11 + 3; 15 = 7 + 5 + 3; 16 = 11 + 5; 17 = 7 + 5 + 3 + 2; 18 = 11 + 7; \\ & 19 = 11 + 5 + 3 \} \end{aligned}$$

zeigen, dass man mit den ersten 5 verschiedenen Primzahlen  $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3 = 5$ ,  $p_4 = 7$  und  $p_5 = 11$  eine Serie von 13 aufeinander folgenden Zahlen bilden kann. Daher hat diese Serie  $Z_0$  die Länge  $|Z_0| = s_0 = 13$ .

Addieren wir die Primzahl  $p_6 = 13$  zu den  $s_0$  Zahlen der Menge  $Z_0$ , so erhalten wir die Menge  $Z_0'$ . Die Vereinigungsmenge aus  $Z_0$  und  $Z_0'$  bezeichnen wir mit  $Z_1$ . Sie hat die Länge  $|Z_1| = s_1 = s_0 + p_6 = 26$ . Wir haben also die 26 Zahlen  $7 = n = 32$  dargestellt.

Durch Addition der Primzahl  $p_7 = 17$  zu den Zahlen  $Z_1$  erhalten wir  $Z_1'$ . Die Vereinigungsmenge von  $Z_1$  und  $Z_1'$ , also  $Z_2$  hat die Länge  $s_2 = s_1 + p_7 = 43$ . Da-

<sup>34</sup> nach Nr. 1, S. 59, 92 – 94; Nr. 3, S. 24 f.

<sup>35</sup> \* 1690 Königsberg, † 1764 Moskau  
Goldbach war Mathematiker und Historiker in St. Petersburg. Er veröffentlichte Arbeiten auf dem Gebiet der Zahlentheorie und korrespondierte mit Euler.

durch erweitern wir die Zahlen, die sich als Summe ungleicher Primzahlen darstellen lassen, auf den Bereich von 7 bis 49.

Dieses Verfahren lässt sich unbegrenzt fortsetzen, wenn in

$$s_{k+1} = s_k + p_{6+k} \text{ stets}$$

$$p_{6+k} = s_k \text{ gilt.}$$

Dies lässt sich durch vollständige Induktion beweisen:

Wenn  $p_{6+k-1} = s_{k-1}$ , so folgt:

$$p_{6+k-1} + p_{6+k-1} = s_{k-1} + p_{6+k-1}$$

$$2p_{6+k-1} = s_{k-1} + p_{6+k-1} = s_k.$$

*Pafnuti Lwowitsch Tschebyscheff*<sup>36</sup> hat 1852 gezeigt, dass für jede natürliche Zahl  $n = 1$  unter den Zahlen  $n + 1, n + 2, \dots, 2n$  wenigstens eine Primzahl vorkommt. Da der Beweis dieses Satzes den Rahmen dieser Arbeit aber überschreitet, möchte ich darauf verzichten.

Eine direkte Folge aus Tschebyscheffs Satz ist, dass das 2-fache einer Zahl stets größer als die der Zahl folgenden Primzahl ist. Es gilt somit:

$$p_{6+k} < 2p_{6+k-1} = s_k \quad \text{q. e. d.}$$

1931 gelang es *Lusternik-Schnirelmann* (1905 – 1938), einem jungen unbekanntem russischen Mathematiker, die Anzahl der Summanden zu begrenzen und zu zeigen, dass jede positive ganze Zahl als Summe von nicht mehr als 300000 Primzahlen dargestellt werden kann. Zwar erscheint dieses Erkenntnis eher belustigend, jedoch war sie ein großer Fortschritt im Beweis der Goldbachschen Vermutungen.

Etwas später schaffte es der russische Mathematiker *Ivan Matveevich Vinogradoff*<sup>37</sup> die Anzahl der Summanden von 300000 auf 4 zu senken. Allerdings ist Vinogradoffs Satz nur für „hinreichend große“ Zahlen bewiesen.

---

<sup>36</sup> \* 1821, † 1894 in Russland

Tschebyscheffs produktivste wissenschaftliche Tätigkeit begann Ende der vierziger Jahre, und beeinflusste die mathematischen Forschung der Folgezeit. Er veröffentlichte Arbeiten auf den Gebieten der Zahlentheorie, Wahrscheinlichkeitsrechnung, Approximationstheorie und Integrationstheorie. In zahlreichen zahlentheoretischen Überlegungen schloss er direkt an die Ergebnisse von Euler an. Aus Überlegungen aus dem Maschinenbau stammen die von ihm erstmals verwendeten Tschebyscheff-Polynome.

<sup>37</sup> \* 1891, † 1983 in Russland

Vinogradoff studierte in St. Petersburg Mathematik. Sein Hauptinteresse galt der Zahlentheorie. Er beschäftigte sich mit Quadratischen Resten, der analytische Zahlentheorie und Primitivwurzeln.

Genauer gesagt bewies er nur, dass es eine Zahl  $N$  gibt, für die gilt, dass jede Zahl  $n > N$  als Summe von höchstens 4 Primzahlen darstellbar ist. Leider lässt dieser Beweis keine Abschätzung von  $N$  zu. Vinogradoff hat also lediglich bewiesen, dass die Annahme, es gäbe unendlich viele ganze Zahlen, die nicht in höchstens 4 Primzahlsummanden zerlegt werden können, zu einem Widerspruch führt.

Die Goldbachsche Vermutung wurde bis heute noch nicht bewiesen, doch konnte sie auch noch nicht durch ein Gegenbeispiel widerlegt werden.

## 9. Anwendung von Primzahlen in der Kryptographie<sup>38</sup>

Abschließend möchte ich nun noch auf die Kryptographie, einem Anwendungsgebiet der Primzahltheorie, zu sprechen kommen.

Mit der fortschreitenden Entwicklung weltweiter Datennetze ist es immer wichtiger geworden, Informationen zu verschlüsseln um sie zu schützen. Eines der verbreitetsten Verfahren hierzu ist die *RSA- Verschlüsselung*. Sie wurde 1977 von *Ronald Rivest*<sup>39</sup>, *Adi Shamir*<sup>40</sup> und *Leonard Adleman*<sup>41</sup> entwickelt. Bei diesem RSA- Verfahren macht man sich ein allbekanntes Problem der Primzahltheorie zunutze. Zwar kann man relativ einfach das Produkt zweier sehr großer Primzahlen bestimmen, aber im nachhinein herauszufinden, welche zwei Zahlen man miteinander multipliziert hat, ist kaum zu bewerkstelligen. Setzt man zum Beispiel für eine Division  $10^{-6}$  Sekunden an, so würde für eine Zahl  $N \sim 10^{100}$  die Ausführung der  $\frac{1}{2}\sqrt{N}$  Divisionen mehr als  $10^{36}$  Jahre dauern. Im

Laufe der Zeit wurden zwar auch raffiniertere Methoden entwickelt, bei denen man mit weniger Divisionen auskommt, aber diese sind ebenfalls in einer Größenordnung, welche die Leistung unserer Computer weit übersteigt.

Beim RSA- Verfahren handelt es sich um ein asymmetrisches Verfahren. Im Gegensatz zum symmetrischen Verfahren, wo Sender und Empfänger einen gemeinsamen Schlüssel haben, hat hier jeder Nutzer einen öffentlichen Chiffrier- und einen privaten Dechiffrierschlüssel. Somit erspart man sich, für

---

<sup>38</sup> nach Nr. 16; Nr. 17; Nr. 5, S. 72

<sup>39</sup> Ronald L. Rivest ist Professor für Electrical Engineering und Computer Science am MIT (Massachusetts Institute of Technology). Er arbeitete intensiv auf den Gebieten der Computer Algorithmen, maschinellen Lernens und VLSI Design. 1986 wurde ihm der Bakerpreis der IEEE verliehen.

<sup>40</sup> Adi Shamir ist heute Professor für Mathematik und Informatik am Weizmann Institute of Science in Rehovot, Israel. Der gebürtige Israeli erhielt für seine wissenschaftlichen Arbeiten auf dem Gebiet der Kryptographie mehrere Auszeichnungen, u.a. den Bakerpreis der IEEE (1986), den UAP Wissenschaftspreis (1990) und die Pius XI Goldmedaille (1993).

<sup>41</sup> Leonard Adleman ist Professor für Computer Science an der University of Southern California in Los Angeles. Er ist der erste Mathematiker gewesen, der DNS für die Datenverarbeitung einsetzte. Er schaffte es, das Problem des Handlungsreisenden (ein Handlungsreisender will eine Anzahl von Städten auf einer optimalen Route nacheinander besuchen) mit Hilfe von DNS-Molekülen zu lösen. Auch er bekam 1986 den Bakerpreis der IEEE verliehen.

jedes potentielle Sender- und Empfängerpaar zwei eigene Schlüssel anzufertigen. Darüber hinaus sind Chiffrier- und Dechiffrierschlüssel vollkommen unterschiedlich, so dass man nicht vom einen auf den anderen schließen kann. Das Produkt der beiden Primzahlen stellt einen Bestandteil des Chiffrierschlüssel dar.

Möchte nun jemand eine Nachricht an einen Nutzer A übermitteln, so codiert er sie mit dem öffentlichen Schlüssel von A. Die so bearbeitete Nachricht kann nun ausschließlich Nutzer A selbst entschlüsseln, da nur er den geheimen Dechiffrierschlüssel kennt.

Das RSA- Verfahren ist momentan weltweit eine der sichersten Verschlüsselungstechniken. Da seine Sicherheit aber hauptsächlich auf dem Problem der Primfaktorzerlegung großer Zahlen beruht, wird es wohl trotzdem über kurz oder lang, spätestens aber mit der Entwicklung besserer und schnellerer Computer, entschlüsselt werden.

## 10. Anhang

### 10.1. Summenregel für unendliche geometrische Reihen

Geometrische Reihe:  $s_n = a_1 + a_1 q^1 + a_1 q^2 + \dots + a_1 q^{n-1}$

$$s_\infty = \frac{a_1}{1-q}$$

hier:  $a_1 = 1$  und  $q = \frac{1}{\rho_1}$

### 10.2. Rechnung 1

$$\begin{aligned} (2^m - 1)(2^{(k-1)m} + 2^{(k-2)m} + \dots + 2^m + 1) &= (2^m - 1)(2^{km-m} + 2^{km-2m} + \dots + 2^m + 1) = \\ &= 2^{km-m+m} + 2^{km-2m+m} + 2^{km-3m+m} + \dots + 2^{2m} + 2^m - \\ &\quad - 2^{km-m} - 2^{km-2m} - \dots - 2^{2m} - 2^m - 1 = \\ &= 2^{km} + 2^{km-m} + 2^{km-2m} + \dots + 2^{2m} + 2^m - \\ &\quad - 2^{km-m} - 2^{km-2m} - \dots - 2^{2m} - 2^m - 1 = \\ &= 2^{km} - 1 \end{aligned}$$

### 10.3. Rechnung 2

$$\begin{aligned} (a+1)(a^{u-1} - a^{u-2} + \dots + a^2 - a + 1) &= \\ &= a^u - a^{u-1} + a^{u-2} - \dots - a^2 + a \\ &\quad + a^{u-1} - a^{u-2} + \dots + a^2 - a + 1 = \\ &= a^u + 1 \end{aligned}$$

Ergänzung:

Auf Grund der abwechselnden Vorzeichen, endet für gerades  $u$  die hintere Klammer immer auf minus 1:  $a^{u-1} - a^{u-2} + \dots - a^2 + a - 1$ . Das absolute Glied 1 wird also subtrahiert. Somit ist

$$\begin{aligned} (a+1)(a^{u-1} - a^{u-2} + \dots - a^2 + a - 1) &= \\ &= a^u - a^{u-1} + a^{u-2} - \dots + a^2 - a + \\ &\quad + a^{u-1} - a^{u-2} + \dots - a^2 + a - 1 = \\ &= a^u - 1 \neq a^u + 1 \end{aligned}$$

F ist folglich nur für ungerade  $u$  auf jeden Fall faktorisiert.

## 10.4. Tabelle der bekannten Mersenneschen Primzahlen

Nr.	Exponent n	Dezimalstellen	Entdeckungsjahr	Entdecker
1	2	1	-----	-----
2	3	1	-----	-----
3	5	2	-----	-----
4	7	3	-----	-----
5	13	4	1456	anonym
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervushin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1279	386	1952	Robinson
16	2203	664	1952	Robinson
17	2281	687	1952	Robinson
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tuckerman
25	21701	6533	1978	Noll & Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson & Slowinski
28	86243	25962	1982	Slowinski
29	110503	33265	1988	Colquitt & Welsh
30	132049	39751	1983	Slowinski
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski & Gage
33	859433	258716	1994	Slowinski & Gage
34	1257787	378632	1996	Slowinski & Gage
35	1398269	420921	1996	Joel Armengaud (GIMPS)
36	2976221	895932	1997	Gordon Spence (GIMPS)
37	3021377	909526	1998	Roland Clarkson (GIMPS)
38	6972593	2098960	1999	Nayan Hajratwala (GIMPS)
39	13466917	4053946	2001	Michael Cameron (GIMPS)

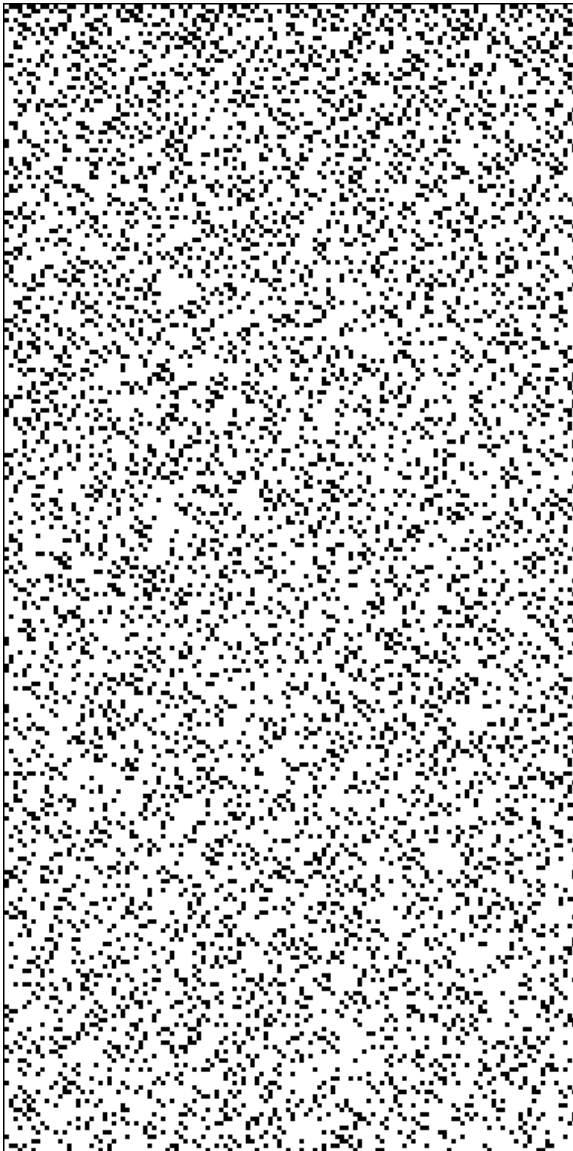
## 10.5. Der Satz von Euler

Sind  $a$  und  $n$  teilerfremd, dann gilt:

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

$\varphi(n)$  ist die Euler'sche Funktion. Sie gibt die Anzahl der zu  $n$  teilerfremden Zahlen kleiner gleich  $n$  an.

## 10.6. Grafische Darstellung aller ungeraden Primzahlen bis 65536



## 11. Literaturverzeichnis

### 11.1. Bücher

**1. Trost, Ernst; Locher - Ernst, L. (Hrsg.):**

Elemente der Mathematik vom höheren Standpunkt aus Bd. 2 – Primzahlen  
2., überarbeitete Auflage  
Basel/ Stuttgart, Birkhäuser Verlag, 1968

**2. Pieper, Herbert:** Mathematische Miniaturen Bd. 2: Zahlen aus Primzahlen -  
Eine Einführung in die Zahlentheorie

2., durchges. u. erw. Auflage mit Anhängen von H. Hasse und H. Reichardt  
Basel - Boston - Stuttgart, Birkhäuser Verlag, 1984

**3. Richard Courant, Herbert Robbins:** Was ist Mathematik?

5., unveränderte Auflage  
Berlin - Heidelberg, Springer-Verlag, 2000

**4. Zagier, Don:** Die ersten 50 Millionen Primzahlen

In: Borho, W., Jantzen, J. C., Kraft, H., Rohlf, J., Zagier, D.: Mathematische  
Miniaturen Bd. 1: Lebendige Zahlen - Fünf Exkursionen  
Basel - Boston - Stuttgart, Birkhäuser Verlag, 1981

**5. Schwarz, Wolfgang:** Über einige Probleme aus der Theorie der Primzahlen  
Stuttgart, Franz Steiner - Verlag - Wiesbaden - GmbH, 1985

**6. Gellert, W., Dr. Küstner, H., Dr. Hellwich, M., Kästner, H. (Hrsg.):**

Kleine Enzyklopädie – Mathematik  
Leipzig, VEB Bibliographische Institut, 1965

### 11.2. Internetadressen

#### 11.2.1. Allgemeines

**7. Beweis von Euler**

<http://www.turing-maschine.de/daten/mathematic/beweise/primenumbers-euler.html>

**8. Primzahlen**

<http://www.mathe.tu-freiberg.de/~hebis/caf/primzahlen.html>

**9. Mersennesche Primzahlen**

<http://home.t-online.de/home/arndt.bruenner/mathe/scripts/mersenne.htm>

**10. Fermatsche Primzahlen**

<http://www.mathe.tu-freiberg.de/~hebis/caf/fermatprim.html>

**11. Zahlentheorie 1**

<http://www.wias-berlin.de/~stephan/thema6.pdf>

**12. Die Primfaktorzerlegung**

[http://www.uni-mainz.de/Schulen/Nieder-Olm/schwerpunkte/projekte/infschul/kr\\_tina.html](http://www.uni-mainz.de/Schulen/Nieder-Olm/schwerpunkte/projekte/infschul/kr_tina.html)

**13. Der Satz von Wilson**

<http://www.zum.de/Faecher/Materialien/dorner/manuskripthtml/kleinerfermat/wilson.html>

**14. Zahlentheorie 2**

<http://www.mathe-seiten.de/zahlentheorie.pdf>

**15. Otto Forster**

<http://www.mathematik.uni-muenchen.de/~forster/primes.html>

**16. Das RSA-Verfahren**

[http://w3.siemens.de/solutionprovider/\\_online\\_lexikon/6/f006736.htm](http://w3.siemens.de/solutionprovider/_online_lexikon/6/f006736.htm)

**17. Der RSA- Algorithmus**

[http://www.uni-mainz.de/Schulen/Nieder-Olm/schwerpunkte/projekte/infschul/kr\\_rsa.html](http://www.uni-mainz.de/Schulen/Nieder-Olm/schwerpunkte/projekte/infschul/kr_rsa.html)

**18. Die Primzahlseite**

<http://home.t-online.de/home/arndt.bruenner/mathe/scripts/primzahlen.htm>

**19. Der Kleine Satz von Fermat**

<http://www.zum.de/Faecher/Materialien/dorner/manuskripthtml/kleinerfermat/kleinerfermat.html>

**11.2.2. Biographien**

**20. Euklid**

<http://utenti.lycos.it/mathematik/mathematiker/Euklid.htm>

**21. Euler**

<http://www.mathe.tu-freiberg.de/~hebisch/cafe/euler.html>

**22. Eratosthenes**

<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Eratosthenes.html>

**23. Mersenne**

<http://utenti.lycos.it/mathematik/mathematiker/mersenne.html>

**24. Fermat 1**

<http://www.mathe.tu-freiberg.de/~hebisch/cafe/fermat.html>

**25. Fermat 2**

<http://utenti.lycos.it/mathematik/mathematiker/fermat.html>

**26. Wilson**

[http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Wilson\\_John.html](http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Wilson_John.html)

**27. Lagrange**

<http://utenti.lycos.it/mathematik/mathematiker/langrange.html>

**28. Gauß**

<http://utenti.lycos.it/mathematik/mathematiker/Gauss.htm>

**29. Hadamard**

<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Hadamard.html>

**30. Vallee – Poussin**

[http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Vallee\\_Poussin.html](http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Vallee_Poussin.html)

**31. Legendre**

<http://utenti.lycos.it/mathematik/mathematiker/legendre.html>

**32. Riemann**

<http://utenti.lycos.it/mathematik/mathematiker/Riemann.htm>

**33. Dirichlet**

<http://utenti.lycos.it/mathematik/mathematiker/dirichlet.html>

**34. Goldbach**

<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Goldbach.html>

**35. Tschebycheff**

<http://finanz.math.tugraz.at/~predota/history/mathematiker/tschebyscheff.html>

**36. Vinogradoff**

<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Vinogradov.html>

**37. Rivest**

<http://www.thg.aa.bw.schule.de/Notizbuch/rsa/rivest.htm>

**38. Shamir**

[http://www.mi.informatik.uni-frankfurt.de/people/merkle/v\\_artikel/node9.html](http://www.mi.informatik.uni-frankfurt.de/people/merkle/v_artikel/node9.html)

**39. Adleman**

<http://www.thg.aa.bw.schule.de/Notizbuch/rsa/adleman.htm>

**40. Biographien bedeutender Mathematiker**

<http://home.t-online.de/home/arndt.bruenner/mathe/Allgemein/bios.htm>

Ich, Susanne Mennecke, erkläre hiermit, dass ich die Facharbeit ohne fremde Hilfe angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel benützt habe.

....., den .....

Ort

Datum

.....

Unterschrift des Schülers