Kleine Sätze und große Geheimnisse

Warum man im Kreis rechnen sollte

Marius Leonhardt, Universität Frankfurt

9. Oktober 2024

Tag der Mathematik, Heidelberg

Plan für heute

Motivation

Modulare Arithmetik

Multiplikation modulo p

Gemeinsames Geheimnis

Motivation

Ein Experiment

Wählen Sie bitte alle

- eine Primzahl p (am besten ≤ 7)
- eine ganze Zahl a, die nicht durch p teilbar ist (am besten $-10 \leq a \leq 10$)

und überprüfen Sie, ob $a^{p-1} - 1$ durch p teilbar ist.

Antwort: immer ja!

Schwarze Magie?

$2^{100} - 1 =$

$$1\,267\,650\,600\,228\,229\,401\,496\,703\,205\,375$$

und $3^{100} - 1 =$

$$515\,377\,520\,732\,011\,331\,036\,461\,129\,765\,621\,272\,702\,107\,522\,000$$

sind ebenfalls durch 101 teilbar.

Kleiner Satz von Fermat

Pierre de Fermat

Satz (Fermat, 18.10.1640)

Sei p eine Primzahl und a eine ganze Zahl, die nicht durch p teilbar ist. Dann ist $a^{p-1} - 1$ durch p teilbar. Anders gesagt: Die Zahl a^{p-1} hat beim Teilen durch p Rest 1. Als Formel:

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

Modulare Arithmetik

Zurück in die Grundschule: Division mit Rest

Wir schreiben

$$a \equiv b \pmod{m}$$

und sagen "*a* ist kongruent zu *b* modulo *m*", falls *a* und *b* beim Teilen durch *m* denselben Rest haben.

- Jede Zahl *a* ist kongruent modulo *m* zu einer der Zahlen

$$0, 1, 2, \ldots, m-2, m-1$$

- $a \equiv b \pmod{m} \iff m$ ist ein Teiler von $a - b$.
- $a \equiv 0 \pmod{m} \iff m$ ist ein Teiler von a.

Rechnen modulo m

Wir können modulo m

- addieren
- subtrahieren
- multiplizieren
- dividieren: nur mit Vorsicht!

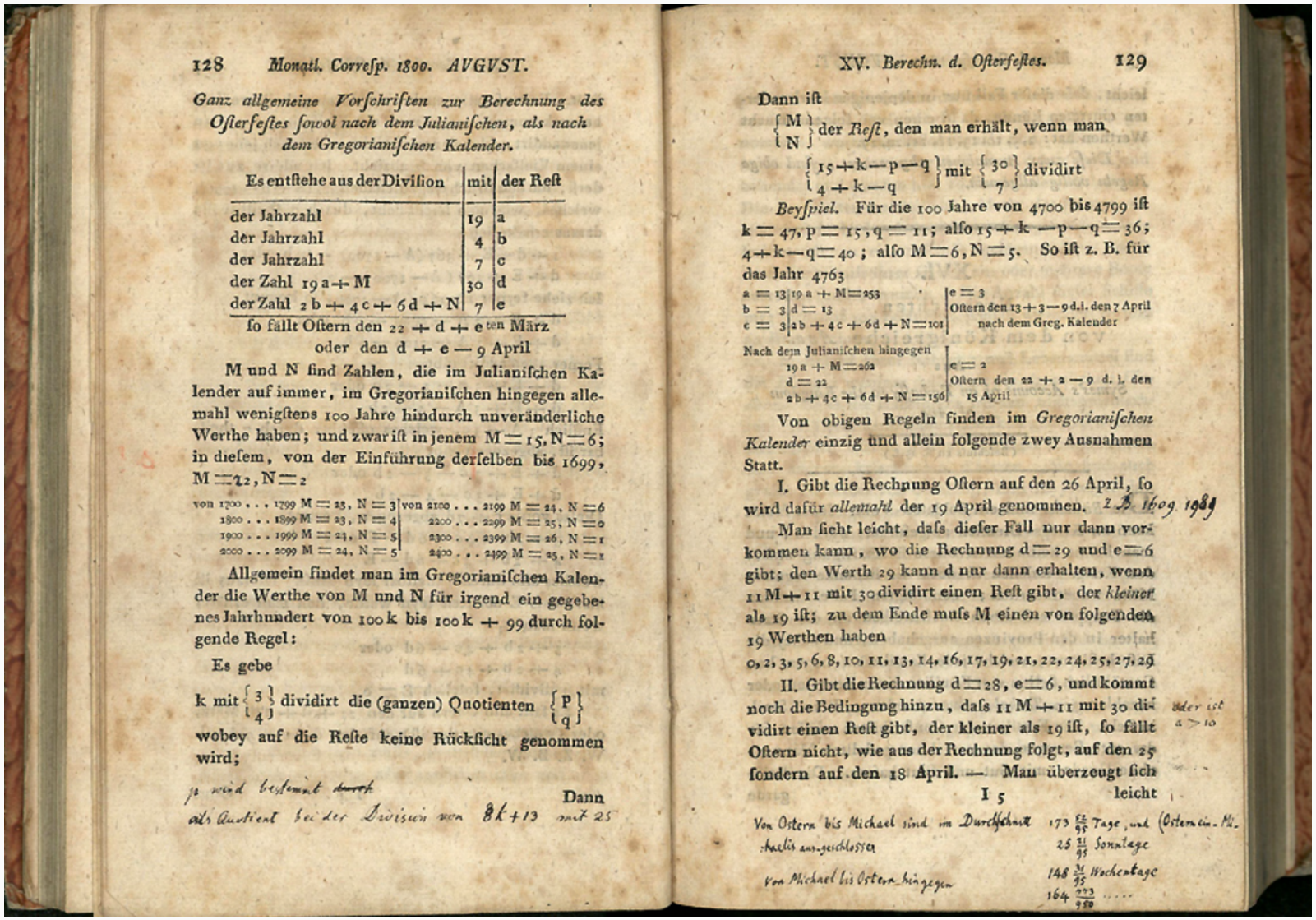
Geburtstagsrechnen

Ist Ihnen schon mal aufgefallen, dass Sie nächstes Jahr genau einen Wochentag später Geburtstag haben als dieses Jahr? Warum ist das so? Weil

$$365 = 52 \cdot 7 + 1 \equiv 1 \pmod 7.$$

Wissen Sie, an welchem Wochentag Sie geboren wurden? Rechnen Sie es aus! (Wer es schon weiß, berechnet stattdessen den Wochentag des 18.10.1640)

Gaußsche Osterformel



128 *Monatl. Corresp. 1800. AVGVST.*

Ganz allgemeine Vorschriften zur Berechnung des Osterfestes sowol nach dem Julianischen, als nach dem Gregorianischen Kalender.

Es entstehe aus der Division	mit	der Rest
der Jahrzahl	19	a
der Jahrzahl	4	b
der Jahrzahl	7	c
der Zahl 19 a + M	30	d
der Zahl 2 b + 4 c + 6 d + N	7	e

so fällt Ostern den 22 + d + e ten März
oder den d + e — 9 April

M und N sind Zahlen, die im Julianischen Kalender auf immer, im Gregorianischen hingegen allemahl wenigstens 100 Jahre hindurch unveränderliche Werthe haben; und zwar ist in jenem M = 15, N = 6; in diesem, von der Einführung derselben bis 1699, M = 22, N = 2

von 1700 . . . 1799	M = 23, N = 3	von 2100 . . . 2199	M = 24, N = 6
1800 . . . 1899	M = 23, N = 4	2200 . . . 2299	M = 25, N = 0
1900 . . . 1999	M = 24, N = 5	2300 . . . 2399	M = 26, N = 1
2000 . . . 2099	M = 24, N = 5	2400 . . . 2499	M = 25, N = 1

Allgemein findet man im Gregorianischen Kalender die Werthe von M und N für irgend ein gegebenes Jahrhundert von 100 k bis 100 k + 99 durch folgende Regel:

Es gebe

k mit $\left\{\begin{matrix}3\\4\end{matrix}\right\}$ dividirt die (ganzen) Quotienten $\left\{\begin{matrix}P\\q\end{matrix}\right\}$

wobey auf die Reste keine Rücksicht genommen wird;

Dann

129 XV. *Berechn. d. Osterfestes.*

Dann ist

$\left\{\begin{matrix}M\\N\end{matrix}\right\}$ der *Rest*, den man erhält, wenn man

$\left\{\begin{matrix}15+k-p-q\\4+k-q\end{matrix}\right\}$ mit $\left\{\begin{matrix}30\\7\end{matrix}\right\}$ dividirt

Beyspiel. Für die 100 Jahre von 4700 bis 4799 ist k = 47, p = 15, q = 11; also 15 + k — p — q = 36; 4 + k — q = 40; also M = 6, N = 5. So ist z. B. für das Jahr 4763

a = 13 | 19 a + M = 253 | e = 3
b = 3 | d = 13 | Ostern den 13 + 3 — 9 d. i. den 7 April
c = 3 | 2 b + 4 c + 6 d + N = 101 | nach dem Greg. Kalender

Nach dem Julianischen hingegen
19 a + M = 262 | e = 2
d = 22 | Ostern den 22 + 2 — 9 d. i. den
2 b + 4 c + 6 d + N = 156 | 15 April

Von obigen Regeln finden im *Gregorianischen Kalender* einzig und allein folgende zwey Ausnahmen Statt.

I. Gibt die Rechnung Ostern auf den 26 April, so wird dafür *allemahl* der 19 April genommen.

Man sieht leicht, dass dieser Fall nur dann vorkommen kann, wo die Rechnung d = 29 und e = 6 gibt; den Werth 29 kann d nur dann erhalten, wenn 11 M + 11 mit 30 dividirt einen Rest gibt, der *kleiner* als 19 ist; zu dem Ende muss M einen von folgenden 19 Werthen haben

0, 2, 3, 5, 6, 8, 10, 11, 13, 14, 16, 17, 19, 21, 22, 24, 25, 27, 29

II. Gibt die Rechnung d = 28, e = 6, und kommt noch die Bedingung hinzu, dass 11 M + 11 mit 30 dividirt einen Rest gibt, der kleiner als 19 ist, so fällt Ostern nicht, wie aus der Rechnung folgt, auf den 25 sondern auf den 18 April. — Man überzeugt sich leicht

I 5

Multiplikation modulo p

Multiplikationstafel

Hier die Multiplikationstafel modulo 11:

	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Sudoku-Muster

Beobachtung/Vermutung

Sei p eine Primzahl. Sei a eine ganze Zahl, die nicht durch p teilbar ist. Dann sind die Zahlen

$$a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a \pmod{p}$$

genau die Zahlen

$$1, 2, 3, \ldots, p-1,$$

nur vielleicht in einer anderen Reihenfolge.

Beweis des Sudoku-Musters

Satz

Die Zahlen $a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a \pmod{p}$ *sind genau die Zahlen* $1, 2, 3, \ldots, p-1 \pmod{p}$, *bis auf Reihenfolge.*

Beweis.

Die Liste $a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a \pmod{p}$ enthält $p-1$ viele Zahlen. Falls zwei dieser Zahlen gleich wären, also $j \cdot a \equiv k \cdot a \pmod{p}$ für $1 \leq j, k \leq p-1$, so wäre

$$0 \equiv ja - ka \equiv (j-k)a \pmod{p},$$

also ist p ein Teiler von $(j-k)a$. Aber p ist kein Teiler von a, also ist p ein Teiler von $j-k$. Aber $-(p-1) \leq j-k \leq p-1$, also folgt $j-k=0$, also $j=k$.

Also enthält $a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a \pmod{p}$ genau $p-1$ verschiedene Zahlen aus $1, 2, \ldots, p-1$, also alle davon. $\square$

Zurück zu Fermat

Pierre de Fermat

Satz (Fermat, 18.10.1640)

Sei p eine Primzahl und a eine ganze Zahl, die nicht durch p teilbar ist. Dann gilt

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

Wir zeigen: Der kleine Satz von Fermat lässt sich aus der "Sudoku-Eigenschaft" folgern!

Beweis des kleinen Satzes von Fermat

Satz (Kleiner Satz von Fermat, Donnerstag 18.10.1640)

Sei p eine Primzahl und $a \not\equiv 0 \pmod{p}$. Dann gilt

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

Beweis.

Wir multiplizieren alle Zahlen $a, 2a, 3a, \ldots, (p-1)a$, also

$$N = a \cdot (2a) \cdot (3a) \cdot \cdots \cdot ((p-1)a) \pmod{p}.$$

Dann gilt einerseits $N \equiv a^{p-1} \cdot (p-1)! \pmod{p}$ und andererseits $N \equiv (p-1)! \pmod{p}$. In der Zeile von $(p-1)!$ steht eine 1, es gibt also eine Zahl e mit $e(p-1)! \equiv 1 \pmod{p}$. Multiplizieren wir $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$ auf beiden Seiten mit e, so erhalten wir $a^{p-1} \equiv 1 \pmod{p}$. □

Blick zurück und nach vorne

Was haben wir benutzt und was gibt es noch zu entdecken?

- Sudoko $\stackrel{\triangle}{=}$ Wir können modulo p durch alles (außer 0) dividieren.
- Es gibt auch ein Verfahren zur schnellen Berechnung der Division modulo p: den Euklidischen Algorithmus.
- Haben damit einen Primzahltest:

$$2^{1234566} \equiv 899557 \pmod{1234567},$$

  also ist 1234567 keine Primzahl.

Gemeinsames Geheimnis

Potenzen modulo m

Wir betrachten die Potenzen von 2 modulo 101, also $2^0 = 1, 2^1 = 2, 2^2 = 4, \ldots, 2^7 = 128 \equiv 27, 2^8 \equiv 54, \ldots, 2^{100} \equiv 1$.
Tatsächlich durchläuft 2^n alle Reste modulo 101.

Vermutung (Artin)

Es gibt unendlich viele Primzahlen p, sodass die Potenzen von 2 alle $p - 1$ Reste modulo p durchlaufen.

Die ersten Primzahlen, für die die Zweierpotenzen alle Reste durchlaufen, sind

$$3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, \ldots$$

Diskreter Logarithmus

Die umgekehrte Frage zum Potenzieren ist z.B.: 2 hoch wie viel ist 73 modulo 101? Wir suchen also n mit

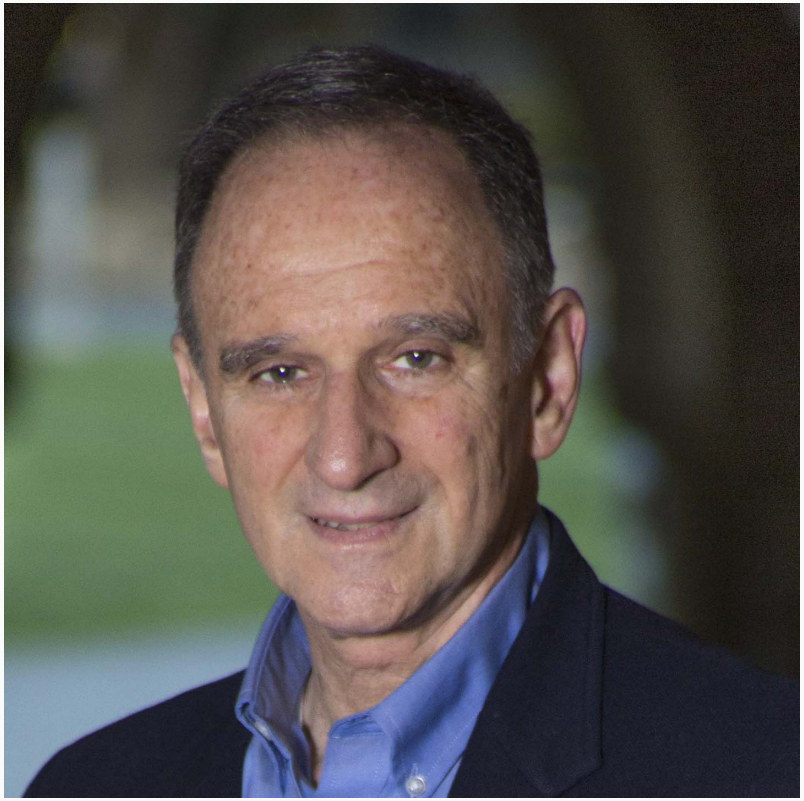
$$2^n \equiv 73 \pmod{101}.$$

Wir nennen n den diskreten Logarithmus von 73 zur Basis 2 modulo 101. Hier $n = 61$.

Es gibt bis heute kein effizientes Verfahren zur Berechnung des diskreten Logarithmus!

Diffie-Hellman-Schlüsselaustausch

Whitfield Diffie



Martin Hellman

Ein gemeinsames Geheimnis

ALICE	UNSICHERER KANAL	BOB
	Primzahl p (z.B. 4096 Bit) Zahl g (z.B. $g = 2$)	
(zufällige) Zahl a $\longrightarrow\longrightarrow\longrightarrow$	$\longrightarrow$ sendet $g^a \pmod p$ $\longrightarrow$ $\longleftarrow$ sendet $g^b \pmod p$ $\longleftarrow$	Zahl b $\longleftarrow\longleftarrow\longleftarrow$
$(g^b)^a \pmod p$		$(g^a)^b \pmod p$

Alice und Bob besitzen nun beide das gemeinsame Geheimnis

$$g^{ab} \pmod p$$

und können dies zur sicheren Kommunikation nutzen.

Fazit

- Beobachtung: $a^{p-1} \equiv 1 \pmod{p}$
- Struktur: Uhrenrechnen (mit p vielen Ziffern auf der Uhr)
- Verständnis der Struktur: Multiplikationstabelle modulo p
- Beweis der Beobachtung
- weitere Anwendungen (Diffie-Hellman) und offene Fragen (Artin)

Vielen Dank fürs Zuhören und Mitdenken!

Gibt es Fragen?

Bonusmaterial

- Slides auf meiner Webseite: `https://www.mathi.uni-heidelberg.de/~mleonhardt/tdm.pdf`
- Klasse Einführung in die Welt der Zahlentheorie: Silverman: A friendly introduction to Number Theory
- Gaußsche Osterformel: `https://www.mathematik.de/osterformel?view=form&chronoform=osterformel&event=submit`
- Kartentrick mittels modularer Arithmetik: `https://www.youtube.com/watch?v=l9dXo5f3zDc`
- Die Zweierpotenzen durchlaufen alle Reste modulo p für `https://oeis.org/A001122`