Durch Zusammenfassen von Summen und Produkten können wir also recht grosse Zahlen bereits im Kopf ausrechen. Wir können sogar Potenzen vereinfachen. Dazu dient der „Kleine Fermat":

> Satz 18 (Kleiner Fermat): Sei $p \in \mathbb{N}$ eine Primzahl und $x \in \mathbb{Z}\setminus\{0\}$ mit $\mathrm{ggT}(x,p)=1$ Dann ist: $x^{p-1} \equiv 1 \bmod p$

Beispiel 55 (Kleiner Fermat):

$p = 2 \Rightarrow 1^{2-1} \equiv 1 \bmod 2$

$p = 3 \Rightarrow \quad 1^{3-1} \equiv 1 \bmod 3$

$2^{3-1} \equiv 4 \equiv 1 \bmod 3$

gcd(5,3) = 1

$3^{5-1} \equiv 1 \bmod 5$

$3^4 \% 5 = 81 \% 5 = 1$ ✓

> Satz 20 (Satz von Euler): Sei $n \in \mathbb{N}\setminus\{0\}$ und $z \in \mathbb{Z}$ mit $\mathrm{ggT}(z,n)=1$. Dann ist $z^{\varphi(n)} \equiv 1 \bmod n$.

2.9 RSA-Verschlüsselung

Die RSA-Verschlüsselung (nach Rivest, Shamir und Adleman) ist ein Public-Key-Verfahren. Funktionsprinzip: Sie vergeben einen öffentlichen Schlüssel, mit dem jeder Botschaften an Sie so verschlüsseln kann, dass nur Sie sie entschlüsseln können.

Beispiel für die Funktionsweise:

i) Wählen Sie zwei Primzahlen p, q, zum Beispiel $p=3$ und $q=11$, und berechnen Sie das Produkt $n = p \cdot q$.

ii) Berechnen Sie $\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)\cdot(q-1) = 20$

iii) Suchen Sie eine Zahl a mit $0 \le a < \varphi(n) = 20$ und mit $\mathrm{ggT}(\varphi(n), a) = \mathrm{ggT}(20, a) = 1$, zum Beispiel $a = 3$

iv) Berechnen Sie das multiplikative Inverse von a in $\mathbb{Z}_{\varphi(n)} = \mathbb{Z}_{20}$:

$a \cdot b \bmod 20 \equiv 1 \Rightarrow b = 7$

v) Veröffentlichen Sie den öffentlichen Schlüssel: $n = 33$, $b=7$

vi) Behalten Sie den privaten Schlüssel $a=3$

vii) Vereinbaren Sie eine Buchstaben Tabelle:

chosen randomly ?

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Nun kann jeder Ihnen verschlüsselte Botschaften schicken, die nur Sie lesen können, weil nur Sie den privaten Schlüssel haben.

$p = 11 \; q = 13 \rightarrow n = 11 \cdot 13 = 143$

$\phi(n) = \phi(p) \cdot \phi(q) = 10 \cdot 12 = 120$

$1 < a < \phi(n) = 120 \qquad \gcd(120, a) = 1$

$a = 23 \qquad a \cdot b \bmod 120 = 1$

$\quad \rightarrow b = 5.26$ ___

if you chose 0 or 1 the inverse is either non existant at 0, or useless → 1 at 1.

Verschlüsseln:

Öffentlicher Schlüssel:	n	33	b	7						
Die Nachricht (Buchstaben B_i):	M	A	T	T	E	R	H	O	R	N
Zahlenwerte der Buchstaben (Zahlen c_i) (nach Buchstabentabelle)	13	1	20	20	5	18	21	15	18	14
Verschlüsseln mit $d_i = c_i^b \bmod n$	7	1	26	26	14	6	2	27	6	20

Beispiele: $13^7 \equiv 7 \bmod 33$, $20^7 \equiv 26 \bmod 33$, $5^7 \equiv 14 \bmod 33$

Übermittelte Nachricht:	7	1	26	26	14	6	2	27	6	20

Entschlüsseln:

Privater Schlüssel:	n	33	a	3						
Empfangene Nachricht (Zahlen d_i):	7	1	26	26	14	6	2	27	6	20
Entschlüsseln mit $e_i = d_i^a \bmod n$	13	1	20	20	5	18	8	15	18	14
Nur ich kann entschlüsseln:	M	A	T	T	E	R	H	O	R	N

Beispiele: $7^3 \equiv 13 \bmod 33$, $26^3 \equiv 20 \bmod 33$, $14^3 \equiv 5 \bmod 33$

Grund für das Funktionieren:

$$e_i \bmod n \equiv d_i^a \equiv \left(c_i^b\right)^a \equiv c_i^{a \cdot b} \equiv c_i^{q \cdot \varphi(n)+1} \equiv c_i$$

Anzahl Dezimalstellen von n	Rechenzeit (Minuten) Mittelwert aus 5 Berechnungen von $\varphi(n)$ min
12	0.00085
13	0.00210
14	0.00595
15	0.02070
16	0.05338
	Geschätzt:
200	4.3 10^{75} Jahre

Code knacken:

i) Berechne Primfaktorzerlegung von n $33 \rightarrow 3 \cdot 11$

ii) Berechne $\varphi(n)$ $2 \cdot 10 = 20$

iii) Berechne Schlüssel a, so dass $a \cdot b \equiv 1 \bmod \varphi(n)$ $21/7 = \underline{\underline{3}}$

iv) $\Rightarrow$ Entschlüsseln

Schwierigkeit: Berechne $\varphi(n)$ für grosse Zahlen n

prime factor $\rightarrow$ $\frac{n}{\text{smallest possible divisor}}$ until you land at primes only !

gcd = greatest common divisor

scm = smallest common multiple

$$\boxed{gcd(a,b) = \max\{d \in N \mid d|a \wedge d|b\}}$$

$$\boxed{scm(a,b) = \min\{m \in N \mid a|m \wedge b|m\}}$$

$$\boxed{scm(a,b) = \frac{a \cdot b}{gcd(a,b)}}$$

Eucledean: $a = b \cdot q + r$

↳ $a = 270$ $b = 192$ $q = ?$ $r = ?$

270 / 192 = 1 remainder 78

$q = 1$ $r = 78$

192 / 78 = 2 remainder 36

78 / 36 = 2 remainder $\boxed{\underline{\underline{6}}}$ gcd

36 / 6 = 6 remainder 0

GCD = 6 → GCD(270, 192) GCD(192, 78)

$\gcd(102, 38)$: reverse

$102 / 38 = 2 \quad r = 26 \qquad 102 = 2 \cdot 38 + 26$

$38 / 26 = 1 \quad r = 12$

$26 / 12 = 2 \quad r = \underline{\underline{2}}$ gcd

$12 / 2 = 6 \quad r = 0$

extended Euclidean algorithm:

$ax \cdot by = \gcd(a, b)$

↳ $\gcd(102, 38) = 2$

reverse the euclidean algorithm (multiplicative inverse ?)

↳ $2 = 26 - 2 \times 12$

↳ $2 = 3 \cdot 26 - 2 \cdot 38$

↳ $2 = 3 \cdot (102 - 2 \cdot 38) - 2 \cdot 38$

↳ $2 = 3 \cdot 102 - 8 \cdot 38$

$x = \underline{\underline{3}} \qquad y = \underline{\underline{-8}}$

We start with our GCD. We rewrite it in terms of the previous two terms:

$$2 = 26 - 2 \times 12.$$

We replace for 12 by taking our previous line ($38 = 1 \times 26 + 12$) and writing it in terms of 12:

$$2 = 26 - 2 \times (38 - 1 \times 26).$$

Collect like terms, the 26's, and we have

$$2 = 3 \times 26 - 2 \times 38.$$

Repeat the process:

$$2 = 3 \times (102 - 2 \times 38) - 2 \times 38.$$

The final result is our answer:

$$2 = 3 \times 102 - 8 \times 38.$$

Thus x and y are 3 and -8.

Definition 32: Zwei natürliche Zahlen $a \in \mathbb{N}, b \in \mathbb{N}$ heissen *teilerfremd*, wenn $\mathrm{ggT}(a, b) = 1$.

Ablauf	x	y	q	r	u	s	v	t
Initialisieren	99	79	1	20	1	0	0	1
1 Wiederholung	79	20	3	19	0	1	1	-1
2 Wiederholung	20	19	1	1	1	-3	-1	4
3 Wiederholung	19	1	19	0	-3	4	4	-5

Dabei verwenden wir die folgende Vorschrift:

Erweiterter Euklidischer Algorithmus

Seien $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$

Initialisierung:

Setze $x = a$, $y = b$, $q = x \operatorname{div} y$, $r = x - y \cdot q$, $(u, s, v, t) = (1, 0, 0, 1)$

(d.h. bestimme q und r so, dass $x = q \cdot y + r$ ist)

Wiederhole bis $r = 0$ ist:

$x = y_{-1}$ $\quad = y$ aus der vorangegangenen Zeile

$y = r_{-1}$ $\quad = r$ aus der vorangegangenen Zeile

$q = x \operatorname{div} y$, $\quad r = x \bmod y = x - y \cdot q$

$u = s_{-1}$ $\quad = s$ aus der vorangegangenen Zeile

$s = u_{-1} - q_{-1} \cdot s_{-1}$ $\quad$ mit u_{-1}, q_{-1}, s_{-1} aus der vorangegangenen Zeile

$v = t_{-1}$ $\quad = t$ aus der vorangegangenen Zeile

$t = v_{-1} - q_{-1} \cdot t_{-1}$ $\quad$ mit v_{-1}, q_{-1}, t_{-1} aus der vorangegangenen Zeile

Ergebnis:

In der letzten Zeile gilt $y = \mathrm{ggT}(a, b) = s \cdot a + t \cdot b$.

Wenn $\mathrm{ggT}(a, b) = 1$ ist, dann folgt: $t \cdot b \equiv 1 \bmod a$

Eulers law

2.8 Der Satz von Euler

Der kleine Fermat kann erfolgreich angewendet werden, um grosse Potenzen zu bestimmen. Der Satz von Euler ist eine Erweiterung davon.

Definition 35 (Eulersche φ -Funktion): Sei $n \in \mathbb{N}$ und $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n | x \text{ hat ein multiplikatives Inverses in } \mathbb{Z}_n\}$. Dann berechnet sich die Eulersche φ -Funktion als

$\varphi(n) =$ Anzahl Zahlen $m \in \mathbb{N}$ mit $1 \le m \le n$ und ggT$(n, m) = 1$

$\varphi(n) =$ Anzahl Elemente $x \in \mathbb{Z}_n$ mit multiplikativem Inversen

$\varphi(n) = |\mathbb{Z}_n^*|$

Beispiel 58:

$\varphi(1) = |\{1\}| = 1$

$\varphi(2) = |\{1\}| = 1$ → 2/2 = 1

$\varphi(3) = |\{1,2\}| = 2$ gcd 2 and 3 = 1

$\varphi(4) = |\{1,3\}| = 2$ gcd 3 and 4 = 1

$\varphi(5) = |\{1,2,3,4\}| = 4$ gcd 5 and 1,2,3,4 = 1

$\varphi(6) = |\{1,5\}| = 2$

$\varphi(7) = |\{1,2,3,4,5,6\}| = 6$ ↓ ......

$\varphi(8) = |\{1,3,5,7\}| = 4$

$\varphi(9) = |\{1,2,4,5,7,8\}| = 6$

$\varphi(10) = |\{1,3,7,9\}| = 4$

$\varphi(11) = |\{1,2,3,4,5,6,7,8,9,10\}| = 10$

$\varphi(12) = |\{1,5,7,11\}| = 4$

Formeln zur Berechnung der Eulerschen φ -Funktion

i) Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist $\varphi(p) = p - 1$

ii) Sei $p \in \mathbb{N}$ eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Dann ist $\varphi(p^n) = p^{n-1} \cdot (p-1)$

iii) Seien $m, n \in \mathbb{N} \setminus \{0\}$ und ggT$(m, n) = 1$. Dann ist $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$