Chinesischer Restklassensatz und RSA

RG, 26.11.2006

Idee:
Der Chinesische Restklassensatz erlaubt es, Multiplikationen mit großen Zahlen auf Multiplikationen mit kleinen Zahlen zu transformieren und die Ergebnisse wieder in den Bereich der großen Zahlen zurückzutransformieren. Genauer: Bei Rechenoperationen mit Zahlen L und M in der Größenordnung einer Zahl n=pq, die aus zwei Primfaktoren p und q zusammengesetzt ist, kann man L und M „hinuntertransformieren" zu kleinen Zahlen r und u, die kleiner als p sind, sowie v und s, die kleiner als q sind. Man führt mit diesen kleineren Zahlen die Rechenoperationen aus und „transformiert" die Ergebnisse „wieder hoch" in den Raum der großen Zahlen bis n. Die Transformationen ihrerseits sind auch nur Rechenoperationen mit den kleineren Zahlen in der Größenordnung von p und q. Die Rücktransformation aus dem kleinen Zahlenraum in den großen besorgt der Chinesische Restklassensatz.

Beispiel: Statt eine Multiplikation mit Zahlen bis 35 auszuführen (zum Beispiel die Multiplikation 17·19 modulo 35), kann man mit Zahlen bis 5 oder 7 rechnen (5 und 7 sind die Primfaktoren von 35), konkret: statt 17·19 modulo 35 genügt es 17 und 19 „hinunterzutranformieren" in die Räume modulo 7 und modulo 5, dann statt „17·19 modulo 35" nur „3·5 modulo 7" und „2·4 modulo 5" zu rechnen, um die Ergebnisse wieder auf den Raum modulo 35 „hochzutransfomieren" (siehe das Beispiel unten).

Hilfssatz:
Für teilerfremde p und q (z.B. verschiedene Primzahlen) gilt: wenn $x \equiv a \pmod p$ und $x \equiv a \pmod q$, dann auch $x \equiv a \pmod{pq}$.

Beweis:
Da x=a+vp und x=a+wq, gilt also a+vp=a+wq, also auch vp=wq. Da p und q teilerfremd sind, müssen die gemeinsamen Teiler dieser Gleichung so verteilt sein: p teilt w und q teilt v. Also gibt es y und z mit w=yp und v=zq. Auf x angewendet ergibt sich also x=a+vp=a+zqp (und übrigens ebenso x=a+wq=a+ypq). Damit ist a ein Rest von x modulo pq.
q.e.d.

Chinesischer Restklassensatz:
Zu teilerfremden p und q (z.B. verschiedene Primzahlen) und zu jedem $a<p$ und $b<q$ gibt es genau ein $x<pq$, das beide Gleichungen erfüllt: $x \equiv a \pmod p$ und $x \equiv b \pmod q$.
x ist „effizient" zu berechnen, d.h. für die Berechnung werden nur Rechenoperationen in der Größenordnung von p und q ausgeführt.

Beweis:
Da p und q teilerfremd sind, gibt es genau ein $u<p$, so dass $uq \equiv 1 \pmod p$. Damit wird x definiert als x:=(a-b)uq+b. Wegen $uq \equiv 0 \pmod q$ ist $x \equiv b \pmod q$. Wegen $uq \equiv 1 \pmod p$ ist $x \equiv a-b+b \equiv a \pmod p$.
x ist eindeutig unter allen Zahlen kleiner als pq (d.h. „eindeutig mod pq"), denn wenn x und x' beide Gleichungen erfüllen, dann ist $x-x' \equiv 0 \pmod p$ und $\pmod q$, also auch $\bmod pq$, da p und q teilerfremd sind. Also sind $x \equiv x' \pmod{pq}$, unter den Zahlen zwischen 0 und pq gibt es nur einen einzigen Vertreter für x und x' modulo pq.
q.e.d.

Komplexität (Rechenaufwand) des Chinesischen Restklassensatzes:
Alle Operationen zur Berechnung der Zahl x<pq, die die Gleichungen x≡a (mod p) und x≡b (mod q) erfüllt, finden nur (mod p) oder (mod q) statt, niemals (mod pq).
Erstens verwendet man zur Bildung des Inversen u von q (mod p) den Euklidischen Algorithmus (mod p), das sind (Größenordnung p) Divisionen mit Rest von q durch p.
Zweitens kostet die Berechnung der Zahl (a-b)uq+b zwei Additionen und drei Multiplikationen in der Größenordnung von q und p.

Vier Beispiele für den Chinesischen Restklassensatz:
(1) Es seien p=7 und q=5. Gesucht wird die Zahl x<5·7=35, die die beiden Gleichungen x≡3 (mod 7) und x≡2 (mod 5) erfüllt:
Erstens die Bildung des Inversen u zu q≡5 (mod 7): Das wird durch u=3 erfüllt, denn uq=3·5=15=1+14≡1 (mod 7).
Zweitens die Berechnung der Zahl x=(a-b)uq+b=(3-2)·15+2=15+2=17.
Das Ergebnis ist offenbar korrekt, denn 17=3+14≡3 (mod 7) und 17=2+15≡2 (mod 5).
(2) Es seien p=7 und q=5. Gesucht wird die Zahl x<5·7=35, die die beiden Gleichungen x≡5 (mod 7) und x≡4 (mod 5) erfüllt:
Erstens wie in Beispiel (1) u=3 und uq=15.
Zweitens x=(a-b)uq+b=(5-4)·15+4=15+4=19.
Das Ergebnis ist offenbar korrekt, denn 19=5+14≡5 (mod 7) und 19=4+15≡4 (mod 5).
(3) Es seien p=7 und q=5. Gesucht wird die Zahl x<5·7=35, die die beiden Gleichungen x≡1 (mod 7) und x≡3 (mod 5) erfüllt:
Erstens wie in Beispiel (1) u=3 und uq=15.
Zweitens x=(a-b)uq+b=(1-3)·15+3=-2·15+3=-27=8-35≡8 (mod 35).
Das Ergebnis ist offenbar korrekt, denn 8=1+7≡1 (mod 7) und 8=3+5≡3 (mod 5).
(4) Übungsaufgabe: Es seien p=7 und q=11. Gesucht wird die Zahl x<7·11=77, die die beiden Gleichungen x≡5 (mod 7) und x≡2 (mod 11) erfüllt.

Satz zur Reduktion der Größenordnung von pq auf p und q bei Multiplikationen:
n=pq sei aus den beiden Primzahlen p und q zusammengesetzt. Dann kann man jeder Zahl M<n ein Tupel (r,s) mit r als Rest von M (mod p) und s als Rest von M (mod q) zuordnen: r:≡ M (mod p), s:≡M (mod q). Umgekehrt kann man jedem Tupel (x,y) mit x<p und y<q mit Hilfe des Chinesischen Restklassensatzes eine eindeutige Zahl Z<pq zuordnen, für die gilt Z≡x (mod p) und Z≡y (mod q).
Diese Zuordnung ist *bijektiv*, verträgt sich mit der *Multiplikation*, und ist ihrerseits von der kleineren *Komplexität p und q* (statt p·q).

Beweis:
Die *Bijektion* ergibt sich aus dem Chinesischen Restklassensatz.
Die *Verträglichkeit mit der Multiplikation* ergibt sich wie folgt:
Gegeben seien L und M, jeweils kleiner als pq und ihre Tupel (u,v) und (r,s), d.h. u≡L mod p, v≡L mod q, sowie r≡M mod p, s≡M mod q. Dann gilt zunächst für das Produkt $LM=(u+u_1p)(r+r_1p)=ur+p(ur_1+u_1r+u_1r_1p)\equiv ur \bmod p$, und mit dem analogen Argument auch ≡ vs mod q, also zerlegt sich das Produkt LM in die Komponenten der Produkte (ur,vs).
Umgekehrt seien Tupel (u,v) für L und und (r,s) für M gegeben, dann ergibt das Tupel (ur,vs) nach dem Chinesischen Restklassensatz gerade die Zahl LM, denn für LM ist LM≡uM≡ur mod p, sowie LM≡vM≡vs mod q.
Dass die Transformationen jeweils nur von der Komplexität der kleinen Primfaktoren p und q ist, liegt an der Konstruktionsmethode des Chinesischen Restklassensatzes (s.o.):

„Hinuntertransformiert“ wird durch einfache Division mit Rest modulo p bzw. modulo q. „Hinauftransformiert“ wird mit der Inversenbildung $uq \equiv 1 \pmod p$, sowie zwei Additionen und drei Multiplikationen mit Zahlen in der Größenordnung von p und q.
q.e.d.

Beispiel für eine Multiplikation mit reduzierter Größenordnung:
Es sei n=35, und es soll die Multiplikation $17 \cdot 19 \pmod{35}$ ausgeführt werden. Wenn man das direkt ausführt, ergibt sich $17 \cdot 19 = 323 = 8 + 9 \cdot 35 \equiv 8 \pmod{35}$.
Mit Hilfe des Chinesischen Restklassensatzes kann die Multiplikation wie folgt in den reduzierten Größenordnungen (mod 5) und (mod 7) ausgeführt werden:
17 wird zerlegt in das Tupel (3,2) mit $17 \equiv 3 \pmod 7$ und $17 \equiv 2 \pmod 5$.
19 wird zerlegt in das Tupel (5,4) mit $19 \equiv 5 \pmod 7$ und $19 \equiv 4 \pmod 5$.
Die Multiplikation der einzelnen Komponenten ergibt
$3 \cdot 5 = 15 = 1 + 14 \equiv 1 \pmod 7$ und $2 \cdot 4 = 8 = 3 + 5 \equiv 3 \pmod 5$.
Das Ergebnistupel (1,3) (mod 7, mod 5) wird nun mit Hilfe des Chinesischen Restklassensatzes wie folgt zum Produkt von $17 \cdot 19 \pmod{35}$ zusammengesetzt: Gesucht ist die Zahl $x<35$, die die Gleichungen $x \equiv 1 \pmod 7$ und $x \equiv 3 \pmod 5$ erfüllt. Diese liefert das Beispiel (3) oben: Erstens die Berechnung des Inversen u von $q \equiv 5 \pmod 7$, das ist offenbar u=3. Zweitens die Bildung von $x = (a-b)uq + b = (1-3)\ 15 + 3 = -30 + 3 = -27 = 8 - 35 \equiv 8 \pmod{35}$. Dieses Ergebnis stimmt mit dem direkt berechneten Ergebnis von $17 \cdot 19 \pmod{35}$ überein.

Effiziente RSA-Verschlüsselung mit Hilfe des Chinesischen Restklassensatzes:
Unter der Voraussetzung, dass man die Primzahlzerlegung n=pq kennt, lässt sich die RSA-Verschlüsselung $c \equiv m^e \pmod n$ mit reduzierter Komplexität (mod p) und (mod q) ausführen. Gegeben Klartextnachricht m, öffentlicher Schlüssel e und Modulus n=pq. Gesucht wird Kryptogramm $c \equiv m^e \pmod n$. Ohne Kenntnis der Zerlegung n=pq wird im Rechenraum der Größenordnung n der Klartext m e-mal mit sich selbst multipliziert. Mit Kenntnis der Zerlegung geht es einfacher:

Vorgehen:
Mit Kenntnis von n=pq zerlegt man m in sein Tupel (m_1,m_2), wobei $m_1 \equiv m \pmod p$ und $m_2 \equiv m \pmod q$. Dann berechne man im kleineren Raum die Gleichungen $c_1 \equiv m_1^e \pmod p$ und $c_2 \equiv m_2^e \pmod q$.
Mit dem Chinesischen Restklassensatz kann man dann c_1 und c_2 auf die Zahl $c<pq$ abbilden (wobei $c \equiv c_1 \bmod p$ und $c \equiv c_2 \bmod q$), für die dann wegen der Verträglichkeit mit der Multiplikation gilt $c \equiv m^e \pmod{pq}$. Das bedeutet, dass c das gesuchte Kryptogramm ist. Analog berechnet man auch die Entschlüsselung $m \equiv c^d \pmod n$, wenn c, d und n=pq gegeben, sowie die Primfaktoren p und q bekannt sind.

Aber Achtung! Die Kenntnis von ***p und q*** bildet eine ***Hintertür zum Knacken des geheimen Schlüssels***. Denn wer p und q kennt, kann zu bekanntem öffentlichen Schlüssel (e, n=pq) den privaten Schlüssel d berechnen, indem er mit dem Euklidischen Algorithmus die Gleichung $de \equiv 1 \pmod{(p-q)(q-1)}$ löst. Einige RSA-Signaturkarten speichern p und q, um mit Hilfe des Chinesischen Restklassensatzes Signaturen und ihre Verifikation effizienter in den kleineren Rechenräumen modulo p und modulo q zu berechnen. Damit bilden diese Signaturkarten aber auch einen Angriffspunkt. Das heißt, sie müssen p und q genau so sicher speichern, wie den privaten Schlüssel d.

