Twierdzenie chińskie o resztach

Wybierzmy dwie liczby względnie pierwsze, na przykład p=5, q = 3. W tabeli poniżej prezentujemy reszty z dzielenia liczb 1,2,...,15 (p*q=15) przez liczby p i q.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

Zauważmy, że każda z liczb N ma inną **parę** reszt z dzielenia przez 3 i 5. Albo odwrotnie: każda para reszt z dzielenia (r,s) wyznacza jedyną liczbę N, dla której **N mod 3 = r** oraz **N mod 5 = s.**

Ponowimy eksperyment dla większej liczby czynników, na przykład p = 2, q = 3, r = 5. Będziemy badać reszty z dzielenia przez te trzy względnie pierwsze liczby dla N=1,....,30 (2*3*5=30)

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
N mod 2	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

N	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
N mod 2	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

Po wnikliwej analizie tych tabel możemy stwierdzić, że żadna **trójka** reszt z dzielenia przez 2, 3 oraz 5 nie powtórzyła się.

Powyższe obserwacje były wykorzystywane do szybkiego sprawdzenia liczby osób w grupie (np. żołnierzy na zbiórce). Jeśli na przykład oddział liczył nie więcej niż 100 żołnierzy, to wystarczyło zarządzić **kolejno odlicz do : 3, 5 i 7**. Skoro 3*5*7 = 105 i jest to liczba większa niż 100, to na podstawie otrzymanych w odliczaniu **reszt z dzielenia przez 3, 5, 7** można było jednoznacznie wywnioskować ilu żołnierzy jest obecnych na zbiórce. Wystarczy posłużyć się tabelami zamieszczonymi poniżej.

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1
N mod 7	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

N	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2
N mod 7	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

N	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
N mod 7	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

N	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4
N mod 7	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

N	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
N mod 3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
N mod 5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
N mod 7	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

Twierdzenie (chińskie o resztach): Jeśli liczby $n_1, n_2, ..., n_k$ są względnie pierwsze oraz liczby $r_1, r_2, ..., r_k$ są dowolnymi liczbami spełniającymi $r_i \in \{0, 1, ..., n_i - 1\}$, to istnieje dokładnie jedno rozwiązanie układu **kongruencji**

$x = r_1 \bmod n_1$

$x = r_2 \bmod n_2$

...

$x = r_k \bmod n_k$

spełniające $0 \le x < n_1 * n_2 * ... * n_k$

Dowód jednoznaczności rozwiązania: Przypuśćmy, że **x** oraz **y** są rozwiązaniami układu kongruencji, czyli

$y \bmod n_1 = x \bmod n_1 = r_1$

$y \bmod n_2 = x \bmod n_2 = r_2$

...

$y \bmod n_k = x \bmod n_k = r_k$

Oznacza to, że

$y - x = 0 \bmod n_1$

$y - x = 0 \bmod n_2$

...

$y - x = 0 \bmod n_k$.

Czyli każda z liczb n_i dzieli różnicę $(y - x)$. Ponieważ

liczby n_i są względnie pierwsze (nie mają wspólnych dzielników),

to również ich iloczyn dzieli $(y - x)$. Dlatego $(y - x) = 0 \bmod n_1 n_2 ... n_k$.

Dowód istnienia rozwiązania: podany poniżej dowód jest konstruktywny, czyli daje algorytm wyznaczania rozwiązania. Oznaczamy liczby $N = n_1 n_2 ... n_k$ oraz $N_i = N / n_i$. Ponieważ liczby n_i są względnie

pierwsze, to NWD(N_i, n_i) = 1. Stosując algorytm Euklidesa znajdujemy liczby całkowite M_i oraz m_i takie, że

$1 = N_i M_i + n_i m_i$, czyli $N_i M_i = 1 - n_i m_i$,

dla $i = 1, 2, ..., k$. Rozwiązanie układu kongruencji jest dane jawnym wzorem

$x = (r_1 N_1 M_1 + r_2 N_2 M_2 + ... + r_k N_k M_k) \bmod N$

Sprawdzamy :

$$\begin{aligned} \boldsymbol{x} \textbf{ mod } \boldsymbol{n_i} &= (r_1 N_1 M_1 + r_2 N_2 M_2 + ... + r_k N_k M_k) \bmod n_i \\ &= r_i N_i M_i \bmod n_i \\ &= r_i(1 - n_i m_i) \bmod n_i = \boldsymbol{r_i} \end{aligned}$$

co kończy dowód twierdzenia.

Przykład:

Rozwiążemy układ kongruencji

```
x mod 3 = 2
x mod 4 = 1
x mod 5 = 4
```

W naszym przypadku $n_1 = 3$, $n_2 = 4$, $n_3 = 5$ oraz $r_1 = 2$, $r_2 = 1$, $r_3 = 4$. Obliczamy liczby N_i

```
N₁ = 4 * 5 = 20
N₂ = 3 * 5 = 15
N₃ = 3 * 4 = 12
```

Korzystając z Algorytmu Euklidesa obliczamy, że

```
1 = NWD (N₁, n₁) = NWD (20, 3) = 7 * 3 - 20
1 = NWD (N₂, n₂) = NWD (15, 4) = 4 * 4 - 15
1 = NWD (N₃, n₃) = NWD (12, 5) = 5 * 5 - 2 * 12
```

Rozwiązaniem jest

```
x = (r₁ N₁ M₁ + r₂ N₂ M₂ + r₃ N₃ M₃) mod (3 * 4 * 5)
  = (2 * (-1) * 20 + 1 * (-1) * 15 + 4 * (-2) * 12) mod 60
  = 29
```

Rzeczywiście, spełnione jest

```
29 mod 3 = 2
29 mod 4 = 1
29 mod 5 = 4
```

Dlaczego RSA działa

Mając do dyspozycji twierdzenie chińskie o resztach i małe twierdzenie Fermata można już łatwo uzasadnić poprawność metody szyfrowania RSA. Przypomnijmy główne składniki tej metody.

1. Wybierz dwie liczby pierwsze p i q
2. Oblicz N = p*q
3. Oblicz F = (p - 1)*(q - 1)
4. Wybierz jakąkolwiek liczbę J (jak jawna), która jest względnie pierwsza z F
5. Oblicz (np. rozszerzonym algorytmem Euklidesa) liczbę T (jak tajna), która spełnia T*J = 1 mod F

Szyfrujemy tak

$$K = W^J \bmod N$$

Deszyfrujemy tak

$$W = K^T \bmod N$$

Aby metoda była rzeczywiście poprawna, musi być spełniona równość

$$W = \left(W^J \bmod N\right)^T \bmod N = w^{J*T} \bmod N$$

Dowód: wiemy, że T*J = 1 mod F, gdyż tak skonstruowaliśmy metodę. Dlatego T*J = 1+k*(p-1)*(q-1) dla pewnej liczby całkowitej k.

Policzymy teraz dwie reszty z dzielenia

$$W^{J*T} \bmod p = W^{1+k*(p-1)*(q-1)} \bmod p =$$
$$\left(W \bmod p * \left(W^{k*(q-1)}\right)^{p-1} \bmod p\right) \bmod p = \left(W \bmod p * a^{p-1} \bmod p\right) \bmod p = W \bmod p$$

Ostatnia równość wykorzystuje małe twierdzenie Fermata dla liczby $a = W^{k*(q-1)}$. W podobny sposób uzasadniamy, że

$$W^{J*T} \bmod q = W^{1+k*(p-1)*(q-1)} \bmod q =$$
$$\left((W \bmod q) * \left(W^{k*(p-1)}\right)^{q-1} \bmod q\right) \bmod q = \left(W \bmod q * b^{q-1} \bmod q\right) \bmod q = W \bmod q$$

przy czym ostatnia równość wykorzystuje małe twierdzenie Fermata dla liczby $b = W^{k*(p-1)}$. Widzimy, że reszty z dzielenia liczby W^{J*T} przez p i q są takie same, jak reszty z dzielenia liczby W. Dlatego, z twierdzenia chińskiego o resztach mamy równość liczb $W = W^{J*T} \bmod (p*q)$.

Zadania

- Rozwiąż układ kongruencji
  x mod 7 = 5
  x mod 11 = 6
- Rozwiąż układ kongruencji
  x mod 5 = 0
  x mod 3 = 2
  x mod 11 = 10
- Rozwiąż układ kongruencji
  x mod 4 = 2
  x mod 9 = 3
  x mod 5 = 1