Kriptografija

Matematičke osnove

dr Slavica Tomović

Univerzitet Crne Gore

Djeljivost

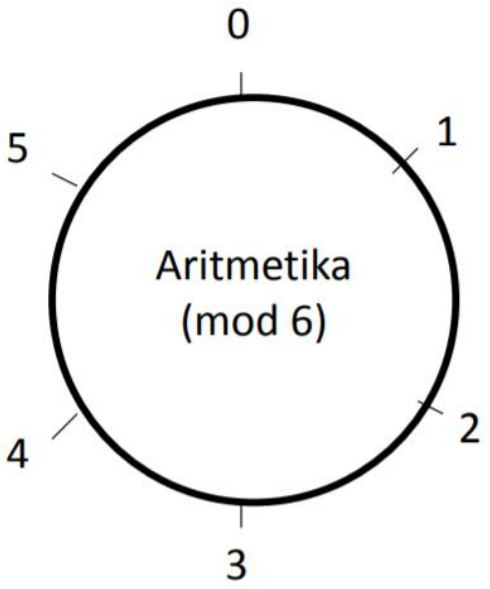
- Kažemo da b dijeli a ako je $a = mb$ za neko m, gdje su a, b, i m cijeli brojevi.
- b dijeli a samo ukoliko nema ostatka pri dijeljenju a/b.
- Notacija $b \mid a$ označava da b dijeli a.

Pozitivni djelioci broja 24 su 1, 2, 3, 4, 6, 8, 12, i 24
13 | 182; - 5 | 30; 17 | 289; - 3 | 33; 17 | 0

- Ako je $a \mid b$ i $b \mid a$, onda je $a = \pm b$.
- Svako $b \neq 0$ dijeli 0.
- Ako je $a \mid b$ i $b \mid c$, onda je $a \mid c$.
- Ako je $b \mid g$ i $b \mid h$, onda je $b \mid (mg + nh)$ za proizvoljne cijele brojeve m i n.

Modularna aritmetika

- Za cijele pozitivne brojeve x i n, x po modulu n predstavlja ostatak dijeljenja x/n.
  - $x \bmod n = r \Rightarrow x = kn + r$, gdje je k neki cio broj.
- Primjeri:
  - $7 \bmod 6 = 1$ ili $7 = 1 \bmod 6$
  - $33 \bmod 5 = 3$ ili $33 = 3 \bmod 5$
  - $33 \bmod 6 = 3$ ili $33 = 3 \bmod 6$
  - $51 \bmod 17 = 0$ ili $51 = 0 \bmod 17$
  - $17 \bmod 6 = 5$ ili $17 = 5 \bmod 6$



Modularna aritmetika

- Koristi se konačan broj vrijednosti i rezultati se dobijaju uvijek u tom skupu vrijednosti.
- Modularna aritmetika je kada se sabiranjem, množenjem i *mod* operacijom redukovanjem dolazi do rešenja.
- Redukovanje je moguće u svakom trenutku:
  - $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
- Primjeri:
  - (12+9) mod 5 = 1
    - ((12 mod 5)+(9 mod 5)) mod 5 = (2+4) mod 5 = 1
  - (3 + 5) mod 6 = 2
  - (2 + 4) mod 6 = 0
  - (7 + 12) mod 6 = 19 mod 6 = 1
    - (7 + 12) mod 6 = (1 + 0) mod 6 = 1

Modularna aritmetika

- Primjer sabiranja po modulu 8:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Modularna aritmetika

- Primjer množenja po modulu 8:

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Modularna aritmetika

- Kongruencija:
  - (a mod n) = (b mod n)
  - zapisuje se kao $a \equiv b \pmod{n}$
  - npr. $100 \equiv 34 \pmod{11}$
- Osobine kongruentnosti:
  - $a \equiv b \pmod{n}$ zahtijeva $n \mid (a-b)$
  - $a \equiv b \pmod{n}$ implicira $b \equiv a \pmod{n}$
  - $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$ implicira $a \equiv c \pmod{n}$

Modularna aritmetika

- Aditivna inverzija x po modu n (označava se sa $-x$) je broj koji treba sabrati sa x da bi modul tog zbira bio 0.
  - $-2 \bmod 6 = 4$ jer je $(2+4) \bmod 6 = 0$
  - Nije negativan broj, samo oznaka!
- Multiplikativna inverzija x po modu n (označava se sa x^{-1}) je broj koji treba pomnožiti sa x da bi modul tog proizvoda bio 1.
  - $3^{-1} \bmod 7 = 5$ jer je $(3 \cdot 5) \bmod 7 = 1$
  - Nije broj manji od 1, samo oznaka!
- Primjeri:
  - $-3 \bmod 6 = 3$
  - $-1 \bmod 6 = 5$
  - $5^{-1} \bmod 6 = 5$
  - $2^{-1} \bmod 6 = ?$
  - Nema svaki broj multiplikativnu inverziju!

Prosti brojevi

- Prost broj je cijeli broj koji ima samo dva djelioca: 1 i samog sebe.
  - Po dogovoru, smatra se da 1 nije prost broj.
  - Primjer prostih brojeva: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...
  - Nema pravila na osnovu kojeg su raspoređeni prosti brojevi u skupu cijelih brojeva.
  - Prostih brojeva ima beskonačno mnogo.
- Svaki cjelobrojan broj $N > 1$ može se faktorisati na jedinstven način:

$$N = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$$

  gdje su $p_1 < p_2 < \ldots < p_n$ prosti brojevi i gdje su e_i pozitivni cijeli brojevi
- Problem faktorizacije broja je u opštem slučaju težak problem.

Prosti brojevi

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Najveći zajednički djelilac (GCD)

- Najveći zajednički djelilac (gcd) cijelih brojeva x i y je najveći broj kojim se mogu podijeliti x i y.
  - $gcd(3, 16) = 1$
  - $gcd(28, 8) = 4$
- Brojevi x i y su **uzajamno prosti** ako je $gcd(x, y) = 1$.
- Dva prosta broja su istovremeno i uzajamno prosta!
- $x^{-1}(mod\ y)$ postoji samo ako su x i y uzajamno prosti.
- $x^{-1}(mod\ y)$ se lako nalazi (ako postoji) korišćenjem Euklidovog algoritma.

Euklidov GCD algoritam

- Efikasan način za pronalaženje *gcd*(*a*,*b*)
- Koristi se teorema: *gcd*(*a*,*b*) = *gcd*(*b*, *a* mod *b*)
- Primjer:

  gcd(2050,1128)

```
2050 = 1 x 1128 + 922      gcd(1128, 922)
1128 = 1 x 922 + 206       gcd(922, 206)
922 = 4 x 206 + 98         gcd(206, 98)
206 = 2 x 98 + 10          gcd(98, 10)
98 = 9 x 10 + 8            gcd(10, 8)
10 = 1 x 8 + 2             gcd(8, 2)
8 = 4 x 2 + 0              gcd(2, 0)
```

```
A=a, B=b
while B>0
    R = A mod B
    A = B, B = R
return A
```

Grupa

- Niz elemenata $A = \{a, b, c, ...\}$ sa nekom binarnom operacijom $*$ čiji je rezultat uvijek u istom nizu elemenata.
- Osobine:
  - *Zatvorenost*: ako su a i b iz A, tada je i $a * b$ iz A.
  - *Asocijativnost*: $(a * b) * c = a * (b * c)$
  - *Ima jedinični element*: $a * e = e * a = a$
  - *Ima inverzni element*: $a * a^{-1} = e$
- Ako je broj elemenata konačan govori se o **konačnoj** grupi i broj elemenata određuje **red grupe**.
- Ako važi komutativnost $a * b = b * a$, onda je to **Abelova grupa**.
- Grupa je **ciklična** ako je svaki element eksponent nekog fiksiranog elementa.
  - $b = a^k$, za neko a i svako b iz grupe.
  - Eksponent definišemo kao višestruku primjenu operacije ($a^3 = a * a * a$).
  - a je u ovom primjeru **generator grupe**.

Prsten

- Niz elemenata sa dvije binarne operacije (sabiranje i množenje)
- Abelova grupa sa operacijom sabiranja
- Za množenje važe:
  - zatvorenost
  - asocijativnost
  - distributivnost nad sabiranjem: $a(b+c) = ab + ac$
- U suštini prsten je skup nad kojim možemo da primjenjujemo sabiranje, oduzimanje i množenje bez da napustimo skup.
- Ako je multiplikativnost komutativna, onda je to **komutativni prsten**.

Polje

- Algebarska struktura u kojoj se mogu izvoditi operacije sabiranja, oduzimanja, množenja i dijeljenja (osim dijeljenja s nulom), i gdje vrijede poznata pravila iz aritmetike običnih brojeva.
  - Sva polja su prsteni, ali ne i obratno.
  - Polja se razlikuju od prstena po tome što se traži da je dijeljenje moguće i da operacija množenja u polju bude komutativna.

Konačna polja

- Galois polja
- Moguće je dokazati da broj elemenata u konačnom polju mora biti stepen prostog broja: p^n.
- Galois polja se obilježavaju sa GF(p^n).
- Najčešće su u upotrebi GF(p) i GF(2^n).
  - Ova polja imaju potpuno drugačiju strukturu!
- GF(p) je niz cijelih brojeva $[0,1,\dots,p-1]$ sa aritmetičkim operacijama po modulu p.
  - Moguće su operacije sabiranja, oduzimanja, množenja i dijeljenja sa rezultatom u skupu GF(p) .

Fermatova teorema

- Ukoliko je p prost broj, a a pozitivni cio broj koji nije djeljiv sa p, onda važi:

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

$a = 7, p = 19$

$7^2 = 49 \equiv 11 \pmod{19}$

$7^4 \equiv 121 \equiv 7 \pmod{19}$

$7^8 \equiv 49 \equiv 11 \pmod{19}$

$7^{16} \equiv 121 \equiv 7 \pmod{19}$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$

- Korisno u testiranju da li je broj prost kod javnih ključeva.

Fermatova teorema

- Alternativna formulacija: Ako je p prost broj, a a je pozitivni cijeli broj, onda je:

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

$p = 5, a = 3 \qquad a^p = 3^5 = 243 \equiv 3 (\text{mod } 5) = a (\text{mod } p)$

$p = 5, a = 10 \qquad a^p = 10^5 = 100000 \equiv 10 (\text{mod } 5) \equiv 0 (\text{mod } 5) = a (\text{mod } p)$

Ojlerova funkcija $\phi(n)$

- ϕ(n) je broj pozitivnih cijelih brojeva manjih od n, koji su uzajamno prosti u odnosu na n.
- Primjeri:
  - $\phi(4) = 2$ jer je 4 uzajamno prost broj sa 1 i 3.
  - $\phi(5) = 4$ jer je 5 uzajamno prost broj sa 1, 2, 3 i 4.
- Kada se radi aritmetika po modulu n, potpuni skup ostatka je: $0 \ldots n-1$.
- Redukovani skup ostatka čine oni brojevi koji su uzajamno prosti u odnosu na n.
  - Npr. za n=10, potpuni skup ostatka je {0,1,2,3,4,5,6,7,8,9}, a redukovani skup ostatka je {1,3,7,9}.
- ϕ(n) predstavlja broj elemenata u redukovanom skupu ostatka.

Neke vrijednosti Ojlerove funkcije $\phi(n)$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Ojlerova funkcija $\phi(n)$

- Za određivanje ϕ(n) potrebna je prosta faktorizacija.
- Ako je p prost broj, onda je $\phi(p)=p-1$.
- Ako su p i q prosti brojevi, onda je: $\phi(pq)=(p-1)(q-1)$.
- Primjeri:
  - $\phi(37) = 36$
  - $\phi(21) = \phi(7 \cdot 3) = (7-1) \cdot (3-1) = 12$
- Ojlerova teorema: Za svako a i n koji su uzajamno prosti važi:

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

- Primjer:
  - a=3; n=10; $\phi(10)=4$;
  - dakle $3^4 = 81 = 1 \bmod 10$

Miller-Rabin algoritam

- Za kriptografske algoritme važno je izabrati na slučajan način jedan ili više prostih brojeva.
- Zadatak je odrediti da li je dati veliki broj prost.
- Algoritam za testiranje neparnog broja *n:*

1. • Pronađi cijele brojeve k, q, gdje je $k > 0$, a q neparno, tako da je $(n-1)=2^k q$;
2. • Odaberi nasumično cijeli broj a, $1 < a < n-1$;
3. • **if** $a^q \bmod n = 1$ **then** return ("možda prost") ;
4. • **for** $j = 1$ **to** $k-1$ **do**
5. • **if** $(a^{2^j q} \bmod n = n-1)$ **then** return ("možda prost") ;
6. • **return** ("nije prost") ;

Miller-Rabin algoritam

- n = 29

$$n - 1 = 2^2 \cdot 7 = 2^k q$$
$$a = 10;$$
$$10^7 \bmod 29 = 17;$$
$$(10^7)^2 \bmod 29 = 28;\ \text{"}možda\ prost\text{"}$$

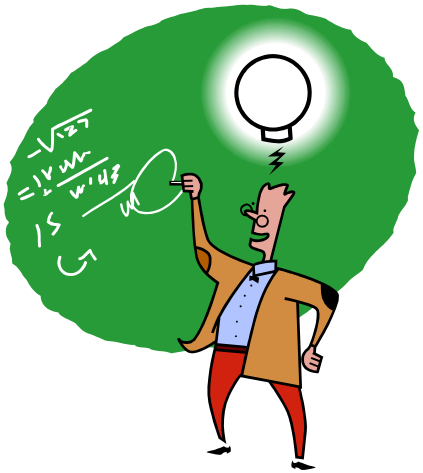
- n = 221

$$n - 1 = 2^2 \cdot 55 = 2^k q$$
$$a = 5;$$
$$5^{55} \bmod 221 = 112;$$
$$(5^{55})^2 \bmod 221 = 200;\ \text{"nije prost"}$$

$$n - 1 = 2^2 \cdot 55 = 2^k q$$
$$a = 21;$$
$$21^{55} \bmod 221 = 200;$$
$$(21^{55})^2 \bmod 221 = 220;\ \text{"možda prost"}$$

Miller-Rabin algoritam

- Vjerovatnoća da za bilo koji neparni broj *n* koji nije prost i za nasumično izabrani *a* algoritam vrati rezultat "*možda prost*" iznosi manje od ¼.
- Za *t* izabranih vrijednosti *a,* vjerovatnoća da svi prođu sa ovim odgovorom je manja od $(\frac{1}{4})^t$.



Primitivni korijeni

- Iz Ojlerove teoreme imamo: $a^{\phi(n)} \equiv 1 \pmod{n}$
- Razmotrimo $a^m \equiv 1 \pmod{n}$, $gcd(a,n)=1$:
  - Mora da važi za $m = \phi(n)$, ali m može biti i manje.
  - Kada stepenovanje dođe do m, ciklus se ponavlja.
- Razmotrimo stepene od 7, po modulu 19:

$$
\begin{aligned}
7^1 &\equiv & &\equiv 7 \pmod{19} \\
7^2 &= 49 = 2 \times 19 + 11 & &\equiv 11 \pmod{19} \\
7^3 &= 343 = 18 \times 19 + 1 & &\equiv 1 \pmod{19} \\
7^4 &= 2401 = 126 \times 19 + 7 & &\equiv 7 \pmod{19} \\
7^5 &= 16807 = 884 \times 19 + 11 & &\equiv 11 \pmod{19}
\end{aligned}
$$

- Sekvenca se ponavlja sa periodom najmanjeg m koje zadovoljava $a^m \equiv 1 \pmod{n}$.

Primitivni korijeni

- Ako je najmanje m= ϕ(n) najmanje m koje zadovoljava $a^m \equiv 1$ (*mod* n), tada se a naziva primitivim korijenom za n.
- Značaj primitivnih korijena ogleda se u tome što ukoliko je a primitivni korijen za n, tada su njegovi eksponenti $\alpha, \alpha^2, \ldots, \alpha^{\phi(n)}$ različiti (po modulu n) i uzajamno prosti sa n.
- Konkretno za prost broj p, za koji je a primitivni korijen, stepeni od a "generišu" grupu po modulu p.
- Nemaju svi cijeli brojevi primitivne korijene.

Primitivni korijeni

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Diskretni logaritmi

- Inverzan problem eksponentizaciji je da se pronađe diskretni logaritam broja po modulu p.
- Podrazumijeva pronalaženje x gdje je $a^x = b \bmod p$, što se zapisuje kao x=$\log_a b$ ili $x = d\log_{a,p}(b)$.
- Jedinstven diskretni logaritam po modulu p i za određenu bazu a postoji samo ako je a primitivni korijen za p.
- Razmotrimo jednačinu:

$$y = g^x \bmod p$$

- Za datko g,x i p, y se jednostavno izračunava.
- Međutim, za zadato y, g i p, u opštem slučaju veoma je teško izračunati x.
  - Kompleknost je približno jednaka kompleksnosti faktorisanja.

Polinomi

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

- Klasična aritmetika sa polinomima:
  - Saberu se ili oduzmu odgovarajući koeficijenti
  - Kod množenja pomnoži se svaki član sa svakim
  - Primjer: $f(x) = x^3 + x^2 + 2$, $g(x) = x^2 - x + 1$
    - $f(x) + g(x) = x^3 + 2x^2 - x + 3$
    - $f(x) - g(x) = x^3 + x + 1$
    - $f(x) \cdot g(x) = x^5 + 3x^2 - 2x + 2$
- Alternativna aritmetika:
  - Aritmetika sa koeficijentima po modulu
  - Modularna aritmetika sa polinomima

Aritmetika nad polinomima sa koeficijentima po modulu

- Kada se izračunava vrijednost svakog koeficijenta, računanje se radi po nekom modulu.
- Koeficijenti polinoma pripadaju konačnom polju *GF*(*p*).
- Najčešće je u upotrebi *mod 2*.
  - Svi koeficijenti su 0 ili 1.
  - Primjer: $f(x) = x^3 + x^2$ i $g(x) = x^2 + x + 1$
    - $f(x) + g(x) = x^3 + x + 1$
    - $f(x) \cdot g(x) = x^5 + x^2$

Modularna aritmetika sa polinomima po modulu

- Svaki polinom se može napisati u formi:
  - $f(x) = q(x)\, g(x) + r(x)$
  - $r(x)$ se može tumačiti kao ostatak
  - $r(x) = f(x)\ mod\ g(x)$
- Ako nema ostatka pri dijeljenju f(x)/g(x) kažemo da g(x) dijeli f(x).
- Ако g(x) nema druge djelioce osime sebe i 1 kaže se da je **nesvodljiv polinom**.
- Euklidov algoritam se može prilagoditi za pronalaženje najvećeg zajedničkog djelioca (GCD) za polinome.
- Polinomijalna aritmetika nam omogućava knstrukciju GF(2^n) polja.
  - Primjena GF(p) sa običnom modularnom aritmetikom u kriptografiji je upitna iz više razloga!
  - GF(2^n) čine **polinomi** sa koeficijentima računatim po modulu 2, čiji je stepen manji od n.

Modularna aritetika sa polinomima u $GF(2^3)$

- Sabiranje:

	+	000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

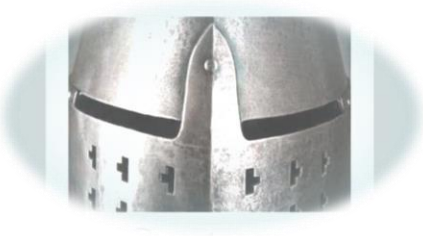
Modularna aritetika sa polinomima u GF(2^3)

- Množenje:
  - Rezultat se računa po modulu sa primitivnim polinom m(x).
  - Primjer: $m(x) = x^3 + x + 1$

	×	000	001	010	011	100	101	110	111
		0	1	2	3	4	5	6	7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

Rezime

- Djeljivost
- Euklidov algoritam
  - Najveći zajednički djelioc
  - Pronalaženje najvećeg zajedničkog djelioca
- Modularna aritmetika
  - Osobine kongruencije
  - Operacije modularne aritmetike
  - Osobine modularne aritmetike
  - Euklidov algoritam sa modularnom aritmetikom
- Prosti brojevi



- Grupa, prsteni, polja
- Konačna polja
- Modularna aritmetika polinoma
- Fermatova teorema
- Ojlerova funkcija
- Ojlerova teorema
- Testiranje prostosti brojeva
  - Miller-Rabin algoritam
- Diskretni logaritmi
  - Primitivni korijeni
  - Logaritmi za modularnu aritmetiku
  - Računanje diskretnih logaritama