WYKŁAD 13

Rozdział 19

Pierścienie, ciała, arytmetyka modularna

19.1 Pierścienie

Definicja 19.1 (Pierścień)**.** Pierścień, oznaczany zwykle przez R, to zbiór z dwoma działaniami $+, \cdot$, spełniającymi warunki:

- $(R, \cdot)$ jest półgrupą (niekoniecznie przemienną)
- $(R, +)$ jest grupą przemienną

Ponadto zachodzi rozdzielność mnożenia względem dodawania

- $a(b+c) = ab + ac$, $(b+c)a = ba + ca$

Pierścień jest *z jednością*, jeśli ma element neutralny dla mnożenia. Pierścień jest *przemienny*, jeśli $ab = ba$ (czyli półgrupa ze względu na mnożenie jest półgrupą przemienną).

Dalej będziemy się zajmować w zasadzie tylko i wyłącznie pierścieniami przemiennymi z jednością.

Definicja 19.2. Ciało $\mathbb{F}$ to pierścień przemienny z jednością, w którym $(\mathbb{F}, \cdot)$ jest grupą, tzn. każdy element ma element odwrotny, oraz elementy neutralne dodawania i mnożenia są różne („$0 \neq 1$”).

Przykład 19.3. Przykłady pierścieni

- liczby całkowite $\mathbb{Z}$
- macierze o współczynnikach z dowolnego ciała (pierścień nieprzemienny!)
- $\mathbb{Z}_m$: liczby modulo m z dodawaniem i mnożeniem
- $R[x]$ wielomiany o współczynnikach z R
- $R[[x]]$ szeregi formalne o współczynnikach z R.

Twierdzenie 19.4. *$\mathbb{Z}_m$ jest ciałem $\iff$ m jest pierwsze.*

Dowód pokażemy w dalszej części rozdziału.

19.2 Arytmetyka modularna $\mathbb{Z}_m$

Definicja 19.5 (Liczenie modulo, $\mathbb{Z}_m$)**.** a przystaje do b modulo m gdy $m|(a-b)$. Oznaczenie:

$$a \equiv_m b \ .$$

Reszta z dzielenia przez m:

$$a \mod m = b \iff a \equiv_m b \wedge b \in \{0, 1, \ldots, m-1\} \ .$$

Przystawanie (modeulo m) jest kongruencją: kongruencję zdefiniujemy dla pierścienia, ale definicja jest analogiczna dla każdej struktury z działaniem.

Definicja 19.6 (Kongruencja (w pierścieniu))**.** Relacja $\equiv \subseteq R^2$ na pierścieniu G jest *kongruencją*, jeśli:

relacja równoważności jest relacją równoważności *oraz*

zachowuje działania zachowuje działania, tzn. dla każdych $a, a', b, b' \in R$ zachodzi:

$$a \equiv b \wedge a' \equiv b' \Rightarrow a \cdot a' \equiv b \cdot b' \wedge a + a' \equiv b + b'$$

Lemat 19.7. *Dla dowolnego $m \in \mathbb{Z}_+$ relacja $\equiv_m$ jest* kongruencją.

- relacja $\equiv_m$

$a \equiv_m b \quad m \mid a-b \quad \exists k \cdot m = a-b$

$a \equiv a \quad m \mid b-a \quad (-k)\cdot m = b-a$

$m \mid 0$

$a \equiv b,\ b \equiv c \Rightarrow a \equiv c$

$a-b = k\cdot m$

$b-c = l\cdot m$

$\hookrightarrow\ a-c = (k+l)m$

$m \mid a-c$

$a \equiv b$

$a' \equiv b' \Rightarrow a+a' \equiv b+b'$

$m \mid a+a'-b-b'$

$= (a-b) + (a'-b')$

$\quad\ \ \| \qquad\ \ \|$

$\quad k\,m \qquad l\,m$

$(k+l)\,m$

$m \mid a\cdot a' - b\cdot b' = a\cdot a' \underbrace{- b\cdot a' + b\cdot a'}_{0} - b\cdot b'$

$= \underbrace{(a-b)\cdot a' + b(a'-b')}_{k\cdot m \qquad\qquad l\cdot m}$

$a'\cdot k\cdot m + b\cdot l\cdot m$

$m(\ldots)$

$a\cdot b \equiv a'\cdot b'$

Wnioski:

1) R, $\equiv$ ← kongruencja moc R

$R/\equiv$ iloraz pierścieniem

2) $R \to R/\equiv \qquad a \mapsto [a]_{\equiv}$ to homomorfizm pierścieni

Ad 1 $\quad R/\equiv$

$$[a]_\equiv + [b]_\equiv = [a+b]_\equiv$$

$$[a]_\equiv \cdot [b]_\equiv = [ab]_\equiv$$

Dobrze zdef.

$$[a] + [b] \qquad [a+b]_\equiv$$
$$\| \qquad \| \qquad \|$$
$$[a'] \qquad [b'] \qquad [a'+b']_\equiv$$
$$a \equiv a' \qquad b \equiv b' \qquad a+b \equiv a'+b'$$

$$(R/\equiv, +, \cdot)$$

$$a(b+c) = ab+ac$$

$$[a]\cdot([b]+[c]) = [a(b+c)]$$

$$[ab+ac] = [ab]+[ac] = [a]\cdot[b] + [a]\cdot[c]$$

$\forall_{a,b,c}$ ~~$\quad$~~ $a(b+c) = ab+ac$

$$a+a+a = 3\cdot a$$

$\mathbb{Z}_3$?

$\mathbb{Z}_2$?

$\forall a \exists b \quad a+a+a \equiv_2 a$? $\quad 1$

$\forall a \exists b \quad b+b=a \vee b+b=a-1$

$\exists \quad b_1, b_2, b_3 \quad b_1 \neq b_2 \wedge b_2 \neq b_3 \wedge b_1 \neq b_3$

$\mathbb{Z}$

$\mathbb{Z}_2$ NIE

$\neg(b_1 = b_2)$

Wniosek 19.8. Przekształcanie $n \mapsto n \bmod m$ jest homomorfizmem pierścieni $\mathbb{Z}$ i $\mathbb{Z}_m$.

To ważne o tyle, że wykonując działania $\bmod m$ możemy dowolnie przełączać się między $\mathbb{Z}$ i $\mathbb{Z}_m$.

W sumie to chcielibyśmy więcej: czy „prawa" przenoszą się między $\mathbb{Z}$ i $\mathbb{Z}_m$? Na pewno nie wszystkie: umiemy powiedzieć, że w $\mathbb{Z}$ są conajmniej 3 różne elementy, ale to nie jest prawda w $\mathbb{Z}_3$. Okazuje się, że prawa się przenoszą, jeśli nie używają negacji.

Definicja 19.9 (Formuła pozytywna)**.** Niech t_1, t_2 będą wyrażaniami zbudowanymi z nawiasów, zmiennych $x_1, x_2, \ldots, x_n$, elementów z A oraz działań $+, \cdot$. Wtedy formuła ψ składająca się spójników $\wedge, \vee$ oraz równości $t_1 = t_2$, gdzie t_1, t_2 są jak wyżej, nazywamy *formuła pozytywną.*

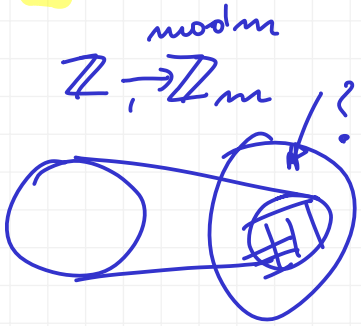
Lemat 19.10. *Niech ψ będzie formuła pozytywną, zaś $\varphi : A \mapsto B$ będzie homomorfizmem na pierścień B.*

Jeśli

$$Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \psi(x_1, x_2, \ldots, x_n)$$

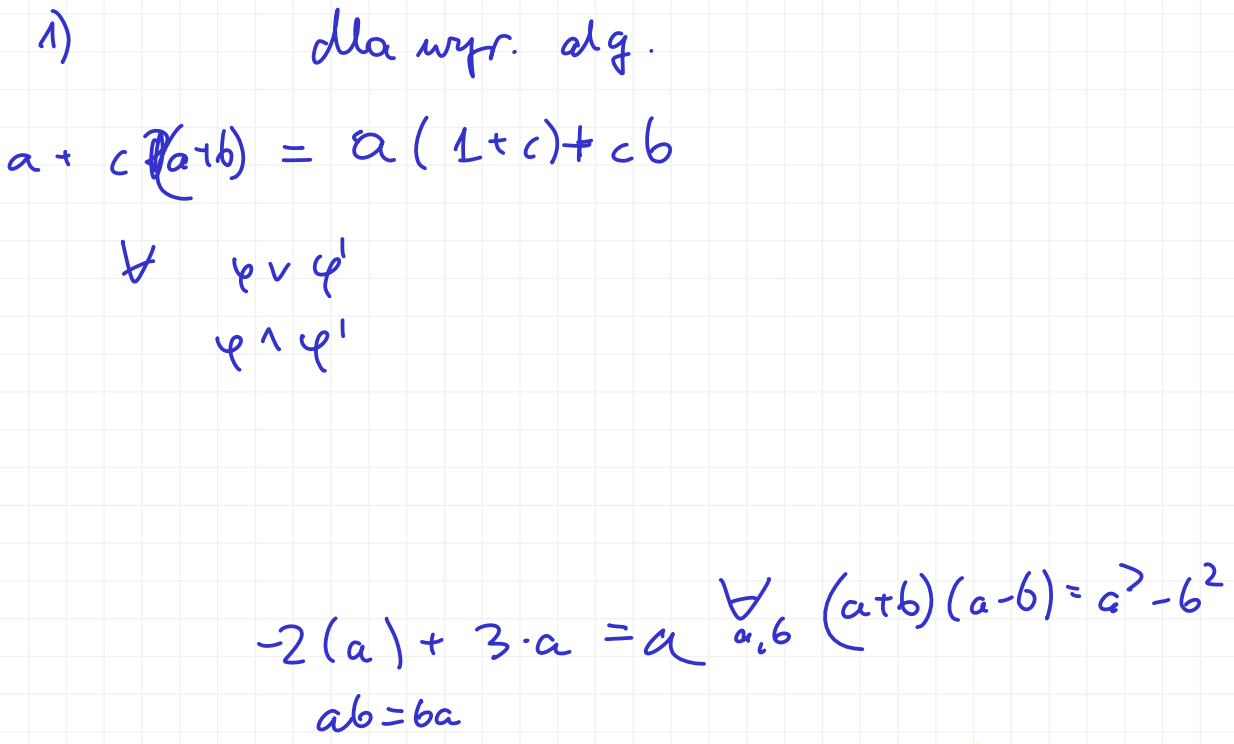
zachodzi w A, to w B zachodzi:

$$Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \psi'(x_1, x_2, \ldots, x_n) \ ,$$



gdzie ψ' jest uzyskane z ψ przez zamianę stałych c w wyrażeniach przez $\varphi(c)$ zaś Q_i jest kwantyfikatorem (uniwersalnym lub egzystencjalnym).

Dowód to indukcja po strukturze. Podstawa indukcji wynika z tego, że to homomorfizm i nie ma negacji.



Wniosek 19.11. W $\mathbb{Z}_m$ zachodzą wszystkie prawa, o których myślimy.

19.3 Algorytm Euklidesa

Wracamy do naszego ulubionego ciała: $\mathbb{Z}_p$. Kiedyś już powiedzieliśmy, że jest tam element odwrotny. A co w $\mathbb{Z}_m$? Jest? Nie ma? Dla którego jest, czy można efektywnie wyznaczyć?

Konstrukcyjna metoda używała będzie *algorytmu Euklidesa*. Opiera się on na obserwacji, że $\gcd(a,b) = \gcd(a-b,b)$ oraz $\gcd(0,b) = \gcd(b,0) = b$. Można to przyspieszyć, poprzez $\gcd(a,b) = \gcd(a \bmod b, b)$.

Definicja 19.12. Liczba $0 \neq k \in \mathbb{N}$ jest największym wspólnym dzielnikiem $a, b \in \mathbb{Z}$, jeśli $k|a$, $k|b$ i dla każdego ℓ zachodzi $\ell|a, \ell|b \implies \ell|k$.

Oznaczenie: $\gcd(a,b)$.

Uwaga. gcd jest największy w sensie porządku częściowego zdefiniowanego przez podzielność.

Lemat 19.13. *Niech $k \neq 0, ab, k \in \mathbb{Z}$. Wtedy:*

1. *Jeśli $k|a$ i $k|b$ to $k|(a+b)$ i $k|(a-b)$.*
2. *Jeśli $k|a$ i $k|b$ to $k|(a \bmod b)$.*
3. *Jeśli $k|(a \bmod b)$ i $k|b$ to $k|a$.*

Algorytm 2 Algorytm Euklidesa

Założenie: a, b są nieujemne, choć jedna jest dodatnia

```
1: while a > 0 oraz b > 0 do
2:     if a < b then
3:         zamień a, b
4:     a ← a − b                          ▷ Może też być a mod b
5: if a ≥ b then
6:     return a
7: else
8:     return b
```

$a \leftarrow a \bmod b$

$k \mid a \quad k \mid b \Rightarrow k \mid a-b, \quad k \mid a \bmod b$

$k \mid b \quad k \mid a-b \Rightarrow k \mid a \qquad k \mid b \wedge k \mid a \bmod b \Rightarrow k \mid a$

Wniosek 19.14. Algorytm Euklidesa zwraca największy wspólny dzielnik.

"$(a,b) \mapsto (a',b)$" to zbiór wspólnych dzielników się nie zmienia

$(a,b) \to \dots \to (0,c)$

dzielniki c c jest $\gcd(0,c)$

Lemat 19.15. *Algorytm Euklidesa (w wersji z modulo) działa w czasie wielomianowym (od długości zapisu liczb). To ograniczenie jest ścisłe.*

Dowód pozostawiamy jako zadanie.

Lemat 19.16. *W czasie algorytmu Euklidesa możemy przechowywane liczby reprezentować jako kombinacje liniowe (o współczynnikach całkowitych) a oraz b.*

(a, b) $\quad \gcd(a,b) = x \cdot a + y \cdot b$

Alg. trzyma a', b' obie dające się wyr. jako komb.

$a' = x \cdot a + y \cdot b \qquad b' = x' \cdot a + y' \cdot b$

$x, y \in \mathbb{Z} \qquad x', y' \in \mathbb{Z}$

Indukcja

$a = 0 \cdot b + 1 \cdot a \qquad b = 0 \cdot a + 1 \cdot b$

$a' \leftarrow a' - b'$

$x \cdot a + y \cdot b \qquad x' \cdot a + y' \cdot b$

$(x - x')a + (y - y') \cdot b$

$a' \leftarrow a' \bmod b'$

$a' - 1 \cdot b'$

---

63 $\qquad$ 48

$\gcd(63, 48)$

$\gcd(15, 48)$

$\gcd(15, 3)$

$\gcd(0, 3)$

63	48
$1 \cdot 63 + 0 \cdot 48$	$0 \cdot 63 + 1 \cdot 48$
1 ; −1	0 ; 1
1 ; −1	−3 ; 4

$\gcd(63, 48) = (-3) \cdot 63 + 4 \cdot 48 = 3$

$-189 + 192 = 3$

To pozwala na

Lemat 19.17. *Dla $a, b \in \mathbb{Z}_+$ istnieją $x, y \in \mathbb{Z}$ takie że*

$$\gcd(a, b) = xa + yb.$$

Dokładnie jedna z tych liczb jest dodatnia i jedna niedodatnia. Dodatkowo, liczby te można wybrać tak, że $|x| < b$, $|y| < a$. Jeśli $\gcd(a, b) = 1$ to są dokładnie dwa takie wyrażenia (w jednym x jest dodatnie a w drugim ujemne).

Proty dowód pozostawiamy jako ćwiczenie.

Lemat 19.18. *W pierścieniu $\mathbb{Z}_m$ element a ma element odwrotny $\iff$ $\gcd(a, m) = 1$.*

$\Leftarrow$ $\quad \gcd(a, m) = 1$

$x \cdot a + y \cdot m = 1$

$x \cdot a = 1 - y \cdot m \quad / \bmod m$

$x \cdot a \equiv_m 1$

$\Rightarrow$ $\quad \gcd(a, m) = b > 1$

$b \mid a \cdot c - l \cdot m$

$(a \cdot c - l \cdot m) = bk \quad / \bmod m$

$a \cdot c \equiv_m b \cdot k$ dla odp l, $k > 1$, $bk < m$

$= a \bmod m$

Uwaga. Zauważmy, że Lemat 19.18 w szczególności daje dowód Twierdzenia 19.4.

$\mathbb{Z}_p \leftarrow$ ciało

19.4 Elementy odwracalne

Definicja 19.19 (elementy odwracalne)**.** Element a pierścienia R nazywamy *odwracalnym*, jeśli istnieje $b \in R$ takie że $ab = 1$.

Zbiór elementów odwracalnych pierścienia R oznaczamy jako R^*.

Twierdzenie 19.20. *Dla dowolnego pierścienia R z jednością zbiór elementów odwracalnych R^* jest grupą na mnożenie.*

$-1, 1 \to 0$

$a \cdot a' = 1$

$(a \cdot b)(b' \cdot a') = 1 \quad b \cdot b' = 1$

Uwaga. $\mathbb{Z}_m^*$ nie ma struktury pierścienia, w szczególności nie jest ciałem!

Twierdzenie 19.21. *Dla ciała skończonego $\mathbb{F}$ grupa $\mathbb{F}^*$ jest cykliczna.*

To twierdzenie jest dość trudne, Rozdział 22 zawiera dowód w przypadku $\mathbb{F} = \mathbb{Z}_p$.

Definicja 19.22 (Symbol Eulera). $\varphi(m)$ to liczba liczb względnie pierwszych z m mniejszych od m.

$\varphi(m) := |\mathbb{Z}_m^*|$

Wniosek 19.23 (Twierdzenie Eulera). Niech a, m są względnie pierwsze. Wtedy

$$a^{\varphi(m)} = 1 \mod m$$

$\mathbb{Z}_m^*$ ← grupa ma mm. $\quad |\mathbb{Z}_m^*| = \varphi(m)$

$a \in \mathbb{Z}_m^* \qquad a^{|\mathbb{Z}_m^*|} \equiv_m 1$

$a < m$

$a^k \bmod m \equiv_m (a \bmod m)^k$

$\varphi(6) = \varphi(2) \cdot \varphi(3)$

Lemat 19.24. *Jeśli n, m są względnie pierwsze, to $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.*

Lemat 19.25. *Jeśli p jest pierwsze, $k > 0$ naturalne, to*

$$\varphi(p^k) = (p-1)p^{k-1} = \frac{p-1}{p} p^k$$

Dowód pozostawiamy jako ćwiczenie.

19.5 Chińskie twierdzenie o resztach

Definicja 19.26 (Produkt pierścieni.). Produkt pierścieni definiujemy standardowo: dla pierścienie R, R' ich produkt $R \times R'$ ma jako zbiór iloczyn kartezjański zbiorów R, R' a działania są po współrzędnych.

$(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$

$R \quad R \times R' \quad R \quad R'$

$\mathbb{Z}_6 \xrightarrow{\text{hom.}} \mathbb{Z}_2 \quad (\text{mod } 2)$

$\mathbb{Z}_6 \to \mathbb{Z}_3 \quad \text{mod } 3$

$\mathbb{Z}_{11 \cdot 13} = \mathbb{Z}_{143}$

$\mathbb{Z}_6 \xrightarrow{\text{hom?}} \mathbb{Z}_2 \times \mathbb{Z}_3$ (isomorf?)

$\mathbb{Z}_{143} \to \mathbb{Z}_{11} \times \mathbb{Z}_{13}$

$\mathbb{Z}_{30} \to \mathbb{Z}_6 \times \mathbb{Z}_5 \Longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$6 \quad 3 \quad 2$

$143 \quad 11 \quad 13$

$30 \quad 6 \quad 5$

Lemat 19.27. *Proste własności:*

- $R \times R$ *i* $R' \times R$ *są izomorficzne*
- *produkt kartezjański jest łączny (z dokładnością do izomorfizmu):* $R_1 \times (R_2 \times R_3)$ *i* $(R_1 \times R_2) \times R_3$ *są izomorficzne*
- *Jeśli* R_1 *jest izomorficzne z* R_1' *a* R_2 *z* R_2'*, to* $R_1 \times R_2$ *jest izomorficzne z* $R_1' \times R_2'$.

Twierdzenie 19.28 (Chińskie Twierdzenie o resztach). *Jeśli $m_1, m_2, \ldots, m_k$ są parami względnie pierwsze, to naturalny homomorfizm z $\mathbb{Z}_{m_1 m_2 \cdots m_k}$ w $\prod_{i=1}^{k} \mathbb{Z}_{m_i}$, gdzie na i-tej współrzędnej bierzemy modulo $\mathbb{Z}_{m_i}$, jest izomorfizmem.*

$m \mapsto (m \bmod m_1, m \bmod m_2, \ldots)$ — izomorfizm; $m_1 \cdot \ldots \cdot m_k$

„na"

Indukcja po k:

1) $k = 2$

2) $\mathbb{Z}_{m_1 \ldots m_{k+1}}$

$$\mathbb{Z}_{m_1 \ldots m_k} \equiv \prod_{i=1}^{k} \mathbb{Z}_{m_i}$$

$m_1 \ldots m_{k+1} = m_1 \ldots m_k \cdot m_{k+1}$

$$\mathbb{Z}_{m_1 \ldots m_{k+1}} \equiv \mathbb{Z}_{m_1 \ldots m_k} \times \mathbb{Z}_{m_{k+1}}$$

$$\equiv \left(\prod_{i=1}^{k} \mathbb{Z}_{m_i} \right) \times \mathbb{Z}_{m_{k+1}}$$

$$\equiv \prod_{i=1}^{k+1} \mathbb{Z}_{m_i}$$

Na?

$\mathbb{Z}_{m \cdot n} \xrightarrow{na}$

$\mathbb{Z}_m \times \mathbb{Z}_n \ni (a, b)$

x

$$\begin{cases} x \bmod m = a \\ x \bmod n = b \end{cases}$$

homomorfizm

$$\begin{cases} x_a \bmod m = 1 \\ x_a \bmod n = 0 \end{cases} \qquad \begin{cases} x_b \bmod m = 0 \\ x_b \bmod n = 1 \end{cases}$$

$$(a \cdot x_a + b x_b) \bmod m = a \cdot \underbrace{x_a}_{1} \bmod m + b \cdot \underbrace{x_b}_{0} \bmod m$$

$$\equiv m \cdot a$$

$$\bmod n \quad b$$

$m, n \rightarrow$ względnie pierwsze

$1 = x \cdot m + y \cdot n$

x_b $(x \cdot m = 1 - yn)$ $(yn = 1 - xm) \rightarrow x_a$

$\downarrow$

$\begin{cases} x_b \bmod m = 0 \\ x_b \bmod n = 1 \end{cases}$ $\begin{cases} x_a \bmod m = 1 \\ x_a \bmod n = 0 \end{cases}$

$(b \cdot x_b + a \cdot x_a)$ $\leftarrow$ moja liczba!

Uwaga. Reprezentacja dużych liczb przy użyciu Chińskiego Twierdzenia o resztach jest jedną z najpraktyczniejszych.

Przykład 19.29. Spróbujmy znaleźć najmniejszą liczbę spełniającą układ równań

$$\begin{cases} x \equiv_{17} 4 \\ x \equiv_{13} 5 \end{cases}$$

Używamy algorytmu Euklidesa, aby znaleźć reprezentację $\gcd(13, 17) = 1$,

17 13 | $1; 0$ | $0; 1$
4 13 | $1; -1$ | $0; 1$
1 | $1; -1$ | $-3; 4$

$4 \cdot 13 = 52$
$3 \cdot 17 = 51$

$1 = 4 \cdot 13 - 3 \cdot 17$

$1 + 3 \cdot 17 = 4 \cdot 13$ mod $17 = 0$
mod $17 = 1$

$-3 \cdot 17 = 1 - 4 \cdot 13$ mod $17 = 0$
mod $13 = 1$

-51 4
5

$5 \cdot (-51) + 4 \cdot 52 = -255 + 208 = -47$

$(-47) + 13 \cdot 17$

Dla układu trzech równań

$$\begin{cases} x \equiv_{17} 4 \\ x \equiv_{13} 5 \\ x \equiv_{11} 2 \end{cases}$$

$-47 + 13 \cdot 17$
reszta mod $13 \cdot 17$

$$\begin{cases} x \equiv_{13 \cdot 17} (-47 + 13 \cdot 17) \\ x \equiv_{11} 2 \end{cases}$$

$\gcd(11, 13 \cdot 17)$

$x_0 \mod 13 = 1$ $\quad x_1 \ldots 0 \quad x_2 \; 0$

$x_0 \mod 11 \cdot 17 = 0$ $\begin{cases} x_0 \mod 17 = 0 \\ x_0 \mod 11 = 0 \end{cases}$ $\quad \mod 13 \cdot 11 \; \begin{matrix} 1 \\ 0 \end{matrix} \quad \mod 13 \cdot 17 \; \begin{matrix} 0 \\ 1 \end{matrix}$

$$4 \cdot x_0 + 5 \cdot x_1 + 2 x_2$$

19.6 Zastosowanie: Algorytm szyfrowania Rabina

Dane: dwie duże (w szczególności: nieparzyste) liczby pierwsze p, q znane właścicielowi. Publicznie znane jest jedynie $n = pq$.

Traktujemy komunikat do zaszyfrowania jako element z $\mathbb{Z}_n$, oznaczamy go jako c (jeśli c jest większe niż n, to dzielimy je na kawałki). Nadawca wiadomości przesyła komunikat $c^2 \bmod n$.

Chcemy pokazać, że:

1. odbiorca umie odtworzyć c z c^2
2. jeśli ktoś umie odtworzyć c z c^2 to umie rozłożyć n na p, q, co uznajemy na trudny problem

$\mathbb{Z}_n \equiv \mathbb{Z}_p^* \times \mathbb{Z}_q$ (w.w. $n = p \cdot q$)

Skorzystamy z silnego twierdzenia, które udowodnimy potem:

Twierdzenie 19.30. *Grupa $\mathbb{Z}_p^*$ jest cykliczna.*

Ile jest liczb, które są kwadratami oraz jakiej są postaci?

Lemat 19.31. *Jeśli p jest liczbą pierwszą, to $a^2 \equiv_p b^2$ wtedy i tylko wtedy, gdy $a \equiv_p b$ lub $a \equiv_p -b$.*

$a^2 \equiv_p b^2 \quad a^2 - b^2 \equiv_p 0 \quad (a-b)(a+b) \equiv_p 0$

W szczególności, w $\mathbb{Z}_p$ dla zadanego c^2 mamy dwa możliwe odszyfrowania: c i $-c$. W $\mathbb{Z}_{pq}$ mamy 4.

Wniosek 19.32. W $\mathbb{Z}_p^*$ jest $(p-1)/2$ kwadratów i $(p-1)/2$ nie-kwadratów. Są to odpowiednio parzyste i nieparzyste potęgi generatora.

Wniosek 19.33. Jeśli g jest generatorem w $\mathbb{Z}_p^*$, to $g^{(p-1)/2} = -1$.

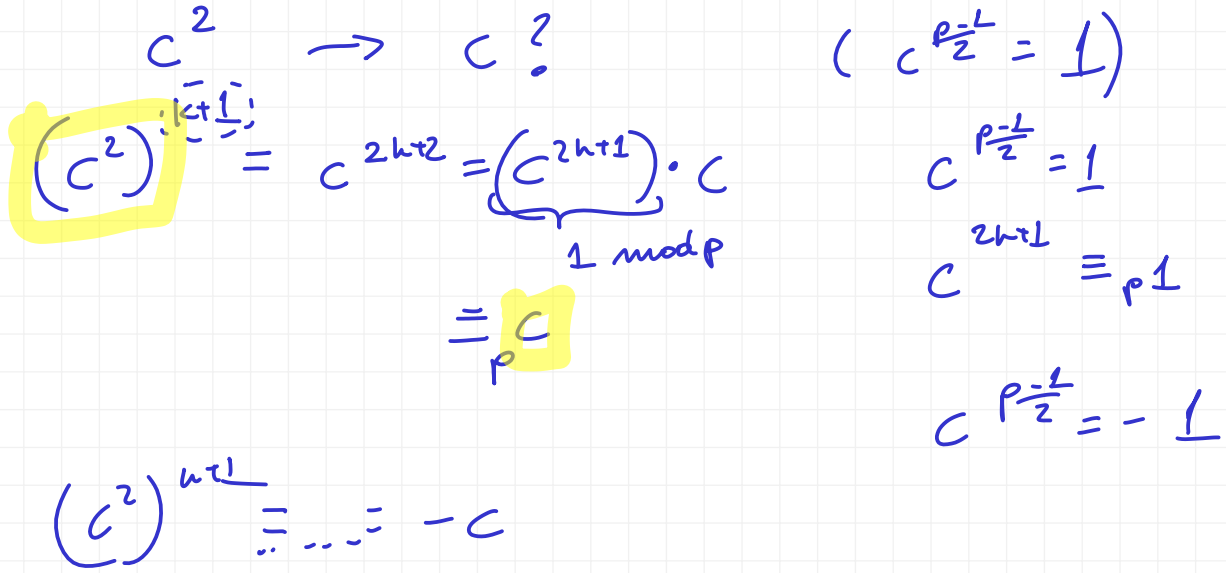
Lemat 19.34. *Jeśli p jest pierwsza to w $\mathbb{Z}_p^*$ jeśli a jest kwadratem, to $a^{(p-1)/2} = 1$, w przeciwnym przypadku $a^{(p-1)/2} = -1$.*

19.6.1 Odtwarzanie

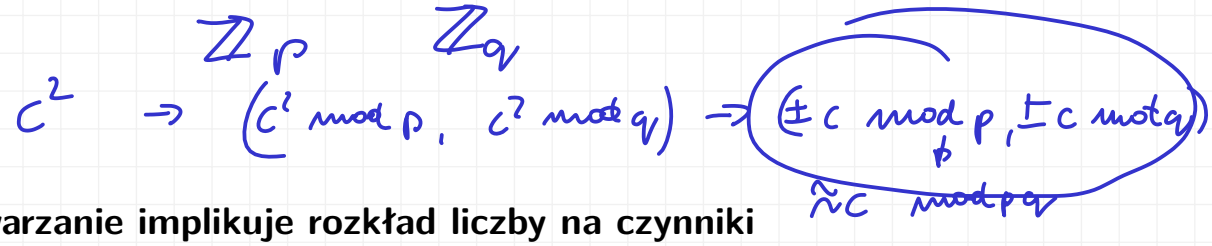
Dla ułatwienia obliczeń, zakładamy, że $p = 3 \bmod 4$, czyli $p = 4k + 3$.

Lemat 19.35. *Dla $c \in \mathbb{Z}_p$ mamy $c^{(p-1)/2} = 1$ lub $(-c)^{(p-1)/2} = 1$*

Bez zmniejszenia ogólności w dalszej części zakładamy, że $c^{(p-1)/2} = 1$, tzn. że z c^2 mając do wyboru $c, -c$ bierzemy to, które jest kwadratem.



Robimy tak dla p, q i tym samym dla n.



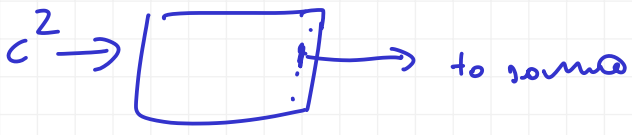
19.6.2 Odtwarzanie implikuje rozkład liczby na czynniki

Zakładamy, że algorytm deszyfrujący jest deterministyczny, tj. dla zadanego m zwróci zawsze ten sam wynik (czyli komunikat c, taki że $c^2 = m$).

Algorytm 3 Algorytm faktoryzujący n używający dekodowania szyfru Rabina

Założenie: $n = pq$, n znane, p, q: liczby pierwsze

1: wylosuj (jednostajnie) $x \in \mathbb{Z}_n^*$
2: oblicz x^2
3: zdekoduj c z $x^2 \bmod n$
4: **if** $c = x$ lub $c = n - x$ **then**
5: wróć do kroku 1
6: wyznacz $p = \gcd((c + x)/2, n)$
7: **return** $(p, n/p)$



Lemat 19.36. *Z prawdopodobieństwem 1/2 otrzymujemy dzielnik n*

x	(x_p, x_q)	$\to (x^2, x^2)$
x'	$(x_p, q - x_q)$	
x''	$(p - x_p, x_q)$	
$n - x$	$(p - x, q - x_q)$	

Co zwróci alg?

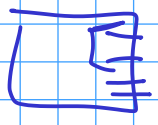
x	x	NIC
x	$n - x$	NIC
x	x'	
	x''	

$$x + x' = (x_p + x_p \bmod p,\ x_q + x_q \bmod q)$$
$$= (0, 2x_q)$$
$$\frac{x + x'}{2} = (0, x_q)$$

dzielę się przez p!

$$\gcd\left(\frac{x + x'}{2}, n\right) = p$$
$$p \mid g' \quad p \nmid q$$

$$\gcd\left(\frac{x + x''}{2}, n\right) = q$$



det.

Wariant losowy

Rozdział 20

Wielomiany

20.1 Pierścień wielomianów

Definicja 20.1 (Wielomian). *Wielomian* f to ciąg $(a_0, a_1, \ldots, a_n)$, myślimy o nich jako o $\sum a_i x^i$. Zwykle zakładamy, że $a_n \neq 0$, w przeciwnym razie dla $n > 0$ utożsamiamy $a_0, \ldots, a_n$ z $a_0, \ldots, a_{n-1}$ (formalnie wielomiany to klasy abstrakcji, ale nie będziemy się tym specjalnie przejmować).

Mnożenie wielomianów definiujemy tak, jak się spodziewamy, tzn. dla wielomianów $(a_0, \ldots, a_n)$ oraz $(b_0, \ldots, b_m)$ ich iloczyn to $(c_0, \ldots, c_{n+m})$, gdzie:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}. \tag{20.1}$$

Zbiór wielomianów o współczynnikach z pierścienia R oraz naturalnym dodawaniem i mnożeniem (tj. po współrzędnych) to *pierścień wielomianów* $R[x]$. *Zerem* w tym pierścieniu jest wielomian (0).

Liczby $a_0, \ldots, a_n$ to *współczynniki wielomianu*, jeśli $a_n \neq 0$ to jest on *współczynnikiem wiodącym*.

Stopień wielomianu $\deg(a_0, \ldots, a_n)$ dla $a_n \neq 0$ to n. W przypadku wielomiany zerowego stopień to $-\infty$.

Zauważmy, że mnożenie takie jak w (20.1) jest dobrze określone nawet dla pier-

ścienia nieprzemiennego. Jeśli myślimy o wielomianach jak o ciągach, to tę operację nazywamy *splotem* dwóch ciągów (i często oznaczamy przez $*$).

Możemy też myśleć że wielomiany to ciągi nieskończone, które mają tylko skończenie wiele niezerowych wyrazów. Wynik mnożenia z dodanymi wiodącymi zerami jest taki sam.

Lemat 20.2 (Poprawność definicji). *$R[x]$ z mnożeniem zdefiniowanym jako splot jest pierścieniem.*

Jeśli R jest pierścieniem przemiennym (z jednością), to $R[x]$ też jest pierścieniem przemiennym (z jednością).

R z jedn. to $1 \cdot x^0$

$f \quad f_0 \dots f_n \qquad g$

$1 \cdot x_0$

$$c_i = \sum_{i=0}^{i} f_i \cdot g_{i-i}^{0} = f_i \cdot g_0^i = f_i$$

$i = i$