Wstęp do teorii liczb z elementami kryptografii

na podstawie wykładu dr. Bartosza Źrałka

Michał Posiadała, Kinga Werońska, Filip Nogaj

Data ostatniej aktualizacji: 13 grudnia 2024

1

Definicja 1.1: Podzielność

Niech $d, a \in \mathbb{Z}$. Mówimy, że d DZIELI/jest WIELOKROTNOŚCIĄ a, jeśli $a = dc$ dla pewnego $c \in \mathbb{Z}$.
Ozn. (d) - zbiór wszystkich wielokrotności d.

Twierdzenie 1.1

Niech $d, a_1, a_2, k \in \mathbb{Z}$.

(i) Jeśli $d|a_1$ i $d|a_2$ to $d|a_1 + a_2$.

(ii) Jeśli $d|a_1$, to $d|ka_1$.

Dowód:

(i) Jeśli $a_1 = dc_1, a_2 = dc_2$, to $a_1 + a_2 = d(c_1 + c_2)$.

(ii) Jeśli $a_1 = dc$, to $ka_1 = dkc$.

Definicja 1.2: Ideał pierścienia $\mathbb{Z}$

IDEAŁEM PIERŚCIENIA $\mathbb{Z}$ nazywamy niepusty podzbiór I zbioru $\mathbb{Z}$ spełniający:

(i) $\underset{a_1, a_2 \in I}{\forall} a_1 + a_2 \in I$,

(ii) $\underset{k \in \mathbb{Z}, a \in I}{\forall} ka \in I$.

Ozn. $I \lhd \mathbb{Z}$

Twierdzenie 1.2: Dzielenie z resztą w $\mathbb{Z}$

Niech $a, b \in \mathbb{Z}, b \neq 0$. Wtedy istnieje dokładnie jedna para liczb całkowitych (q, r) spełniająca

$$a = bq + r, \qquad 0 \leqslant r < |b|.$$

Dowód:
Załóżmy, że $b > 0$ i rozważmy $W = \{bx : x \in \mathbb{Z}, bx \leqslant a\}$ i poczyńmy kilka obserwacji:

- $W \subset \mathbb{Z}$
- W jest ograniczone z góry (przez a)
- $W \neq \emptyset$

Niech $bq = \max W$. Weźmy $r = a - bq$. Skoro $bq \in W$, to $bq < a$, czyli $\frac{r}{a-bq} \geqslant 0$. Ponadto $b(q+1) = bq + b > bq$, a skoro $bq = \max W$, to $b(q+1) \notin W$. Innymi słowy $b(q+1) > a$ tzn. $b > \underbrace{a - bq}_{r}$.

Załóżmy, że $b < 0$. Najpierw dzielimy a przez $-b$:

$$a = -b \cdot \tilde{q} + \tilde{r} \text{ dla } \tilde{q}, \tilde{r} \in \mathbb{Z}, 0 \leqslant \tilde{r} < -b$$

$$a = b \cdot (-\tilde{q} + \tilde{r})$$

$$q := -\tilde{q} \quad r := \tilde{r} \quad 0 \leqslant |b|$$

Pozostaje wykazać jednoznaczność pary (q, r).
Załóżmy, że są dwie takie pary $(q_1, r_1), (q_2, r_2) \in \mathbb{R}^2$ które spełniają

$$a = bq_i + r_i, \qquad 0 \leqslant r_i \leqslant |b| \text{ dla } i = 1, 2$$

$$bq_1 + r_1 = q_2 + r_2$$
$$|b(q_1 - q_2)| = |r_2 - r_1| < |b|$$
$$|b(q_1 - q_2)| < |b|$$

Jako że $b \neq 0$, dzielimy przez $|b|$:

$$|q_1 - q_2| < 1$$

Skoro $q_1, q_2 \in \mathbb{Z}$, to z tego wynika, że $q_1 = q_2$, a z tego wynika, że $r_1 = r_2$, udowodniliśmy więc jednoznaczność.

Twierdzenie 1.3

Niech $I \lhd \mathbb{Z}$. Wtedy $I = (d)$ dla pewnego d.

Dowód:
Możemy założyć, że $I \neq (0)$. Wtedy $I \cap \mathbb{N} \neq \emptyset$, bo istnieje $a \in I, a \neq 0$. Z własności ideału, $(\pm 1) \cdot a \in I$.
Niech $d = \min(I \cap \mathbb{N})$. Pozostaje uzasadnić, że $I = (d)$.

- Inkluzja $(d) \subseteq I$ jest oczywista, bo $d \in I$.
- Niech $a \in I$. Chcemy pokazać, że $a \in (d)$. Mamy

$$r = \underbrace{a}_{\in I} - \underbrace{dq}_{\in I}$$

  Z def. d otrzymujemy $r = 0$, tzn. $a = dq \in (d)$.

Definicja 1.3: Ideał generowany

Dla $a_1, ..., a_k \in \mathbb{Z}$ zdefiniujmy

$$(a_1, ..., a_k) := \{l_1 a_1 + ... + l_k a_k, l_i \in \mathbb{Z}\}$$

Jest to najmniejszy (w sensie inkluzji) ideał zawierający $a_1, ..., a_k$. Nazywamy go Ideałem Generowanym.

Twierdzenie 1.4

Niech $a, b \in \mathbb{Z}$. Wtedy

1. $a|b \iff (b) \subseteq (a)$
2. $(a) = (b) \iff a = \pm b$

Dowód:

(i) $(b) \subseteq a \iff b \in (a) \iff \underset{c \in \mathbb{Z}}{\exists} b = ac \iff a|b$

(ii)

$$(a) = (b) \iff \begin{cases} (a) \subseteq (b) \\ (b) \subseteq (a) \end{cases} \iff \begin{cases} b|a \\ a|b \end{cases} \iff b = ka = klb, \quad k, l \in \mathbb{Z} \iff$$
$$\iff b(kl - 1) = 0$$

Z czego wynika, że $a = \pm b$.

Definicja 1.4: Największy Wspólny Dzielnik

Niech $a_1, ..., a_k \in \mathbb{Z}$. Niech $d \in \mathbb{Z}_{\geqslant 0}$ spełnia:

(i) $d|a_1, ..., d|a_k$,

(ii) jeśli $d' \in \mathbb{Z}_{\geqslant 0}$ spełnia $d'|a_1, ..., d'|a_k$ to $d'|d$.

Wtedy nazywamy d Największym Wspólnym Dzielnikiem i oznaczamy

$$d = NWD(a_1, ..., a_k).$$

Twierdzenie 1.5

Dla ustalonego zestawu $a_1, ..., a_k \in \mathbb{Z}$, $NWD(a_1, ..., a_k)$ istnieje i jest wyznaczone jednoznacznie.

Dowód:

1. Istnienie
   Rozważmy $I = (a_1, ..., a_k)$. Na podstawie Twierdzenia 1.1 wiemy, że istnieje takie $n \in \mathbb{N}$, że $I = (n)$. Weźmy $d = |n|$. Chcemy pokazać, że d spełnia założenia NWD.

   (i) $(a_i) \subseteq (a_1, ..., a_k) = (d)$,
   więc z twierdzenia 1.4 $d|a_i$ dla $i = 1, ..., k$

   (ii) Niech $d' \in \mathbb{Z}_{\geqslant 0}$, $d'|a_i$ dla $i = 1, ..., k$. Zatem $a_i \in (d')$, więc $(d) = (a_1, ..., a_k) \subseteq (d')$ czyli $d'|d$ z twierdzenia 1.4.

2. Jedyność
   Jeśli d_1 i d_2 spełniają definicję NWD, to

$$\left.\begin{matrix} d_1|d_2 \\ d_1|d_2 \end{matrix}\right\} \implies d_1 = d_2$$

Wniosek 1.1

Niech $a_1, ..., a_k \in \mathbb{Z}$. Wtedy istnieją $x_1, ..., x_k$ takie, że $NWD(a_1, ..., a_k) = x_1a_1 + ... + x_ka_k$.

Dowód:
$NWD(a_1, ..., a_k)$ jest nieujemnym generatorem ideału $(a_1, ..., a_k)$, którego każdy element jest wyżej wymienionej postaci.

2

Twierdzenie 2.1: istnienie i jedyność NWW liczb całkowitych

Niech $a_1, ..., a_k \in \mathbb{Z}$. Istnieje dokładnie jedna liczba $m \in \mathbb{Z}_{\geqslant 0}$ taka, że:

(i) $a_1|m, ..., a_k|m$,

(ii) jeśli $m' \in \mathbb{Z}_{\geqslant 0}, a_1|m', ..., a_k|m'$, to $m|m'$.

Liczbę m nazywamy NAJMNIEJSZĄ WSPÓLNĄ WIELOKROTNOŚCIĄ i oznaczamy $NWW(a_1, ..., a_k)$.

Dowód:
Istnienie:
Weźmy m - nieujemny generator ideału $(a_1) \cap ... \cap (a_k)$.

(i) $m \in (a_1) \cap ... \cap (a_k) \subset (a_i)$, więc $a_i|m$ dla $i = 1, ..., k$

(ii) Załóżmy, ż $a_1|m', ..., a_k|m'$. Innymi słowy $m' \in (a_1), ..., m' \in (a_k)$. Zatem $m' \in (a_1) \cap ... \cap (a_k) = (m)$. Stąd $m|m'$.

Jedyność:
Jeśli m_1, m_2 spełniają warunki (i) i (ii), to $m_1|m_2$ i $m_2|m_1$, więc $m_1 = m_2$.

Definicja 2.1: liczby względnie pierwsze

Liczby całkowite a, b nazywamy WZGLĘDNIE PIERWSZYMI, jeśli $NWD(a, b) = 1$.

Twierdzenie 2.2: Bachet

Weźmy $a, b, c \in \mathbb{Z}$. Niech a i b będą względnie pierwsze oraz niech $a|bc$. Wtedy $a|c$.

Dowód:
Z wniosku 1.1 możemy napisać $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$. Stąd $c = xac + ybc$, co jest podzielne przez a.

Definicja 2.2: liczba pierwsza

Liczbę $p \in \mathbb{N}, p \geqslant 2$ nazywamy LICZBĄ PIERWSZĄ, jeśli jej jedynymi dzielnikami naturalnymi są 1 i p.
Ozn. $\mathbb{P}$ - zbiór wszystkich liczb pierwszych

Lemat 2.1

Niech $p \in \mathbb{P}, a, b \in \mathbb{Z}$ i $p|ab$. Wtedy $p|a$ lub $p|b$.

Dowód:
Przypuśćmy, że $p \nmid a$. Wtedy $NWD(p, a) = 1$ (bo $NWD(p, a)|p$, więc $NWD(p, a) = 1$ lub $NWD(p, a) = p$, a jeśli $NWD(p, a) = p$, to $p = NWD(p, a)|a$).
Wobec tego $p|b$ z twierdzenia 2.2.

Wniosek 2.1

Niech $p \in \mathbb{P}, a_1, ..., a_k \in \mathbb{Z}, p|a_1 \cdot ... \cdot a_k$. Wtedy $p|a_i$ dla pewnego $i = 1, .., k$.

Dowód:
Indukcja ze względu na k:

1. dla $k = 1$ oczywiste

2. Przypuśćmy, że wniosek zachodzi dla $k \in \mathbb{N}$.
   Niech $p \in \mathbb{P}, a_1, ..., a_{k+1} \in \mathbb{Z}$ oraz $p|a_1 \cdot (a_2 \cdot ... \cdot a_{k+1})$. Z lematu 2.1 $p|a_1$ lub $p|(a_2 \cdot ... \cdot a_{k+1})$. Wobec tego, z założenia indukcyjnego, $p|a_1$ lub $p|a_2$ lub...lub $p|a_{k+1}$.

Twierdzenie 2.3

Każdą liczbę naturalną $n > 1$ można rozłożyć na iloczyn liczb pierwszych. Taki rozkład jest jednoznaczny (z dokładnością do kolejności czynników).

Dowód:
Istnienie - indukcja ze względu na n:

1. $n = 2 \in \mathbb{P}$
2. Załóżmy, że $n \in \mathbb{N}, n > 2$ oraz, że każda liczba naturalna $m, 1 < m < n$ rozkłada się na iloczyn liczb pierwszych. Jeśli n jest pierwsze, to szukanym rozkładem jest $n = n$. Załóżmy więc, że $n \notin \mathbb{P}$. Wtedy $n = n_1 n_2$, gdzie $n_1, n_2 \in \mathbb{N}, 1 < n_1, n_2 < n$.

   Z założenia indukcyjnego $n_1 = \prod_{p \in \mathbb{P}} p^{\alpha_p}, n_2 = \prod_{p \in \mathbb{P}} p^{\beta_p}$.

   Wtedy $n = n_1 n_2 = \prod_{p \in \mathbb{P}} p^{\alpha_p + \beta_p}$.

Jednoznaczność - indukcja ze względu na n:

1. $n = 2$ - rozkład jednoznaczny w postaci iloczynu liczb pierwszych
2. Niech $n \in \mathbb{N}, n > 2$. Załóżmy, że rozkład na iloczyn liczb pierwszych każdej liczby naturalnej $1 < m < n$ jest jednoznaczny z dokładnością do kolejności czynników.

   Załóżmy, że $n = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k} = p_1^{\beta_1} \cdot ... \cdot p_k^{\beta_k}$, gdzie $p_i \in \mathbb{P}$, $p_i \neq p_j$ dla $i \neq j$ oraz $\alpha_i, \beta_i \in \mathbb{Z}_{\geqslant 0}$ (mogą być zerowe).

   Skoro $n > 1$, to nie wszystkie $\alpha_1, ..., \alpha_k$ są zerowe. BSO załóżmy, że $n_1 \geqslant 1$. Wtedy $p_1|n$.

   Mamy zatem $p_1| \underbrace{(p_1 \cdot ... \cdot p_1)}_{\beta_1 \text{ czynników}} \cdot ... \cdot \underbrace{(p_k \cdot ... \cdot p_k)}_{\beta_k \text{ czynników}}$.

   Z wniosku 2.1, gdyby $\beta_1 = 0$, to mielibyśmy $p_1|p_j$ dla $j \neq 1$, co daje $p_1 = p_j$, a to jest sprzeczność.

   Zatem $\beta_1 \geqslant 1$. W takim razie $p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_k^{\alpha_k} = \frac{n}{p_1} = p_1^{\beta_1 - 1} \cdot p_2^{\beta_2} \cdot ... \cdot p_k^{\beta_k}$.

   Z założenia indukcyjnego ($\frac{n}{p_1} < n$) otrzymujemy:

   $\alpha_1 - 1 = \beta_1 - 1 \Leftrightarrow \alpha_1 = \beta_1$,
   $\alpha_2 = \beta_2$,
   .
   .
   .
   $\alpha_k = \beta_k$.

Uogólnienie dla pierścienia $A \in \{\mathbb{Z}, K[X], \mathbb{Z}[i]\}$:

- definicja podzielności pozostaje taka sama
- dzielenie z resztą w A:

  Dla $a, b \in A, b \neq 0$ istnieją $q, r \in A$ spełniające $a = bq + r$ oraz $N(r) < N(b)$, gdzie dla $u \in A$

$$N(u) = \begin{cases} |u| \text{ dla } A = \mathbb{Z}, \\ |u|^2 = \bar{u}u \text{ dla } A = \mathbb{Z}[i], \\ 2^{deg(u)} \text{ dla } A = K[X]. \end{cases}$$

3

Definicja 3.1

Elementy $a, b \in A$ nazywamy STOWARZYSZONYMI (co zapisujemy $a \sim b$), jeśli $a = ub$, gdzie $u \in A^*$ (grupy elementów odwracalnych pierścienia A).

Grupy elementów odwracalnych pierścienia $A \in \{\mathbb{Z}, K[X], \mathbb{Z}[i]\}$:

- $\mathbb{Z}^* = \{-1, 1\}$
- $K[X]^* = K^* = K$
- $\mathbb{Z}[i]^* = \{-i, i, -1, 1\}$
  Zauważmy bowiem, że jeśli $a \in \mathbb{Z}[i]^*$ to $ab = 1$ dla pewnego $b \in \mathbb{Z}[i]$. Stąd $N(a)N(b) = N(1) = 1$. Jedynymi elementami $\mathbb{Z}[i]$ mającymi normę 1 są $-i, i, -1, 1$. Przy czym te elementy są odwracalne w $\mathbb{Z}[i]$. (Widzimy, że jeśli $N(a) = 1$ to $a^{-1} = \bar{a}$.)

W tym wykładzie A zawsze oznacza jeden z trzech wymienionych powyżej pierścieni. Jeśli dowody twierdzeń są pominięte, oznacza to, że są analogiczne do dowodu dla Z.

Lemat 3.1

Niech $a, b \in A$. Wówczas:

(i) $a|b \Leftrightarrow (b) \subset (a)$

(ii) $(a) = (b) \Leftrightarrow a \sim b$

Twierdzenie 3.1

W pierścieniu A każdy ideał jest główny. Mówimy, że A jest PIERŚCIENIEM IDEAŁÓW GŁÓWNYCH (w skrócie po polsku PIG).

Dowód:
Niech $I \lhd A$. Jeśli $I \neq (0)$ to pokazujemy, że element o najmniejszej dodatniej normie w I jest generatorem I.

Twierdzenie 3.2: Największy Wspólny Dzielnik w A

Niech $a_1, ..., a_k \in A$. Istnieje dokładnie jeden element $d \in A$, z dokładnością do stowarzyszenia pierścienia A, spełniający:

(i) $d|a_1, ..., d|a_k$,

(ii) jeśli $d' \in A$ spełnia $d'|a_1, ..., d'|a_k$ to $d'|d$.

Ten element d oznaczamy $NWD(a_1, ..., a_k)$.

Twierdzenie 3.3: Najmniejsza Wspólna Wielokrotność w A

Niech $a_1, ..., a_k \in A$. Z dokładnością do stowarzyszenia istnieje dokładnie jeden element $m \in A$ taki, że:

(i) $a_1|m, ..., a_k|m$,

(ii) jeśli $m' \in A, a_1|m', ..., a_k|m'$, to $m|m'$.

Ten element m oznaczamy $NWW(a_1, ..., a_k)$.

Twierdzenie 3.4

Niech $a, b \in A, a|bc, NWD(a, b) \sim 1$. Wówczas $a|c$.

Definicja 3.2

Element $a \in A, a \neq 0, a \notin A^*$ nazywamy NIEROZKŁADALNYM jeśli jedynymi (z dokładnością do stowarzyszenia) dzielnikami a są 1 i a.

Twierdzenie 3.5

Niech γ będzie elementem nierozkładalnym pierścienia $A, a, b \in A, \gamma|ab$. Wtedy:
$\gamma|a$ lub $\gamma|b$

Uwaga 1:
Element $\gamma \in A, \gamma \neq 0, \gamma \notin A^*$ spełniający warunek: $\forall\, a, b \in A : \gamma|ab \Rightarrow \gamma|a \vee \gamma|b$ nazywamy elementem pierwszym. Zatem powyższe twierdzenie można sformułować tak:
Każdy element nierozkładalny pierścienia A jest pierwszy.

Uwaga 2:
W dowolnej dziedzinie całkowitości każdy niezerowy element pierwszy jest nierozkładalny. W szczególności w naszym pierścieniu A zbiór wszystkich elementów nierozkładalnych to zbiór wszystkich elementów pierwszych.

Niech γ będzie pierwszy w dziedzinie całkowitości D, $\gamma = ab$, gdzie $a, b \in D$. Z definicji $\gamma|a \vee \gamma|b$. Przypuśćmy, że $\gamma|a \Rightarrow a = \gamma c$, gdzie $c \in D$. Wówczas:
$\gamma = \gamma cb \Rightarrow 1 = cb$

Wniosek 3.1

Niech γ będzie nierozkładalny w A i niech $a_1, ..., a_k \in A$ takie, że $\gamma|a_1 \cdot ... \cdot a_k$.
Wtedy $\gamma|a_i$ dla pewnego i.

Twierdzenie 3.6: Jednoznaczność rozkładu w A

Niech $a \in A, a \neq 0, a \notin A^*$. Element a można zapisać jednoznacznie z dokładnością do kolejności czynników i ich stowarzyszenia w postaci iloczynu elementów nierozkładalnych.

Dowód:
Dowód przebiega analogicznie do dowodu tego twierdzenia dla $A = \mathbb{Z}$, z indukcją ze względu na $N(a)$.

- W $\mathbb{Z}$ zbiór wszystkich elementów nierozkładalnych to $\{\pm p : p \in \mathbb{P}\}$
- Opiszmy zbiór wszystkich elementów nierozkładalnych w $\mathbb{Z}[i]$.
  Niech $\gamma \in \mathbb{Z}[i]$ będzie nierozkładalne.
  Zauważmy, że $\gamma|\gamma\bar{\gamma} = N(\gamma)$ przy tym: $N(\gamma) \in \mathbb{N}, N(\gamma) > 1$. $N(\gamma)$ możemy rozłożyć w $\mathbb{Z}$ na iloczyn liczb pierwszych. Wobec tego $\gamma|p$ dla pewnego $p \in \mathbb{P}$. Zauważmy, że γ nie może dzielić dwóch różnych $p, q \in \mathbb{P}$. Mielibyśmy bowiem: $\gamma|NWD(p, q) = 1$. Pozostaje opisać jak $p \in P$ rozkłada się w $\mathbb{Z}[i]$.

Uwaga ogólna:
Jeśli $a \in \mathbb{Z}[i], N(a) \in \mathbb{P}$ to a jest nierozkładalne w $\mathbb{Z}[i]$.
$a = bc$
$\mathbb{P} \ni N(a) = N(b)N(c) \Rightarrow N(b) = 1 \vee N(c) = 1$
Czyli:
$b \in A^* \vee c \in A^*$

- $2 = i(1-i)^2$, gdzie $i \in \mathbb{Z}[i]^*$
  $(1-i)$ jest nierozkładalne w $\mathbb{Z}[i]$ ponieważ $N(1-i) = 2 \in \mathbb{P}$

Dowód:
Niech $p \in \mathbb{P} \setminus \{2\}$. Załóżmy, że $p\alpha \cdot \beta$, gdzie α nierozkładalne. Wtedy

$$\underbrace{N(p)}_{p^2} = \underbrace{N(\alpha)}_{\neq 1} \cdot N(\beta)$$

Zatem są dwie możliwości

1. Albo $N(\alpha) = p^2, N(\beta) = 1$ co oznacza, że $\beta \in \mathbb{Z}[i]^*$ czyli $p \sim \alpha$. W szczególności p nierozkładalne
2. Albo $N(\alpha) = p$
   Niech $\alpha = a + ib, a, b \in \mathbb{Z}$
   Otrzymujemy $\alpha\overline{\alpha} = p$, tzn $p = a^2 + b^2$
   Zauważmy, że $a^2 + b^2 \mod 4 \in \{, 1, 2\}$

$$0^2 \equiv 0(4) \qquad 1^2 \equiv 1(4) \qquad 2^2 \equiv 0(4) \qquad 3^2 \equiv 1(4)$$

   Mamy, że dla $p \equiv 3(4)$ zachodzi przypadek 1), czyli takie p jest nierozkładalne w $\mathbb{Z}[i]$.

Pozostaje przypadek $p \equiv 1(4)$. Zauważmy że zachodzi następujące twierdzenie:

Twierdzenie 3.7

Dla każdego $p \in \mathbb{P}$, $p \equiv 1(4)$ istnieje $x \in \mathbb{Z}$ spełniający

$$x^2 \equiv -1(p)$$

Zaaplikujmy powyższe twierdzenie do $p \equiv 1(4)$. Weźmy $x \in \mathbb{Z}, x^2 \equiv -1(p)$. Innymi słowy $p|(x^2 + 1) \iff p|(x - i)(x + i)$ w $\mathbb{Z}[i]$.
Zauważmy, że $NWD(p, x + i) \not\sim 1, p$

- $NWD(p, x + i) \not\sim 1$
  W.p.p z tw. Barcheta mielibyśmy $p|(x - i)$ SPRZECZNOŚĆ
- $NWD(p, x - i) \not\sim p$
  Analogicznie, w.p.p z tw. Barcheta mielibyśmy $p|(x + i)$ SPRZECZNOŚĆ

Napiszemy $NWD(p, x + i) \sim a + bi$.
Skoro $NWD(p, x + i) \not\sim 1$, to $a + ib \notin \mathbb{Z}[i]^*$
Stąd $N(a + ib) > 1$

- $a + ib|p, p = (a + ib) \cdot \gamma, \quad \gamma \in \mathbb{Z}[i]$
  Zatem $N(a + ib)|N(p) = p^2$. Pozostają dwie możliwości:

$$N(a + ib) = p \vee N(a + ib) = p^2$$

  Jeśli $N(a + ib) = p^2$ to $N(\gamma) = 1$, czyli $\gamma \in \mathbb{Z}[i]^*$.
  Mielibyśmy $a + ib \sim p$,przez co $NWD(p, x + i) \not\sim p$.
  Pokazaliśmy więc, że $N(a+ib) = p$. Oznacza to, że $p = (a+ib)(a-ib)$, a skoro $N(a+ib) = p \in \mathbb{P}$, to $a - ib$ oraz $a + ib$ są nierozkładalne.
  Zauważmy jeszcze, że $a + ib \not\sim a - ib$
  W szczególności $a + ib|a - ib$
  Oczywiście $a + ib|a + ib$
  Stąd $a + ib|a - ib + (a + ib) = 2a$
  Bierzemy normy: $p = N(a + ib)|N(2a) = 4a^2$
  Podobnie $a + ib|(a + ib) - (a - ib) = 2ib, \qquad p|N(2ib) = 4b^2$
  Skoro $p \in \mathbb{P} \setminus \{2\}$ to $p|a \wedge p|b$ to

$$a + ib = p(a' + ib')$$
$$a - ib = p(a' - ib')$$
$$p = p^2(a' + ib')(a' - b'i)$$
$$1 = p(a'^2 + b'^2)$$

4

Wniosek 4.1

Każdą liczbę $p \in \mathbb{P}, p \equiv 1(4)$ można zapisać jako $a^2 + b^2$ dla pewnych $a, b \in \mathbb{Z}$. To przedstawienie jest jedyne, z dokładnością do znaku i permutacją a z b.

Wynika to z jednoznaczności rozkładu $(a + bi)(a - ib)$ z dokładnością do kolejności czynników nierozkładalnych i ich stowarzyszenia, czyli z dokładnością do $\pm 1, \pm i$.

Metoda 4.1: wyznaczania $p = x^2 + y^2$

1. Znajdź $x \in \mathbb{Z}$, t. że $x^2 \equiv -1(p)$
2. Oblicz $NWD(p, x + i)$ w $\mathbb{Z}[i]$ za pomocą algorytmu Euklidesa.
3. $NWD(p, x + i) \sim a + ib$
4. $p = a^2 + b^2$

Konstrukcja pierścienia ilorazowego R/I:
Zakładamy, że R jest przemienny i z 1.
I - ideał pierścienia R ($I \lhd R$).

Stwierdzenie 4.1

Relacja $\equiv$ w $\mathbb{R}$ określona $a \equiv b \iff a - b \in I$ jest relacją równoważności. Klasę równoważności elementu a oznaczamy $[a]_I$.

Dowód:

- zwrotność
$$a - a = 0 \in a \implies a \equiv a$$
- symetryczność
$$a \equiv b \iff a - b \in I \iff (-1)(b - a) \in I \iff b \equiv a$$
- przechodniość
$$\left.\begin{matrix} a \equiv b \\ b \equiv c \end{matrix}\right\} \implies \left.\begin{matrix} a - b \in I \\ b - c \in I \end{matrix}\right\} \implies a - b + b - c \in I \implies a - c \in I \iff a \equiv c$$

5

Stwierdzenie 5.1

Określmy następujące działania w R/I:

- $[a] + [b] = [a + b]$
- $[a] \cdot [b] = [ab]$
- $1_{R/I} = [1_R]$
- $0_{R/I} = [0_R]$

Tak określone działania są poprawne i czynią z R/I pierścień przemienny z 1.

Dowód:

1. Dodawanie w R/I jest dobrze określone, tzn. nie zależy od wyboru reprezentantów klas.
   Niech $a_1, a_2, b_1, b_2 \in R$, $[a_1] = [a_2]$, $[b_1] = [b_2]$. Chcemy pokazać, że $[a_1 + b_1] = [a_2 + b_2]$, tzn. że $a_1 + b_1 = a_2 + b_2$.
   Mamy $a_1 + b_1 - (a_2 + b_2) = a_1 - a_2 + b_1 - b_2$, gdzie $a_1 - a_2 \in I$ (bo $a_1 \equiv a_2$) oraz $b_1 - b_2 \in I$ (bo $b_1 \equiv b_2$). Zatem $a_1 + b_1 - (a_2 + b_2) \in I$.

2. Mnożenie w R/I jest dobrze określone.
   Niech $a_1, a_2, b_1, b_2 \in R$, $[a_1] = [a_2]$, $[b_1] = [b_2]$. Tym razem mamy pokazać, że $[a_1 b_1] = [a_2 b_2]$.
   Mamy $a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2)$. Wiemy, że $b_1 - b_2 \in I$ (bo $b_1 \equiv b_2$) i analogicznie $a_1 - a_2$. Zatem $a_1(b_1 - b_2) \in I$ oraz $b_2(a_1 - a_2) \in I$. Czyli finalnie $a_1 b_1 - a_2 b_2 \in I$, a co za tym idzie $a_1 b_1 \equiv a_2 b_2$ tzn. $[a_1 b_1] = [a_2 b_2]$.

Stwierdzenie 5.2

Niech $n \in \mathbb{N}$. Moc $\mathbb{Z}/(n)$ (ozn. $\mathbb{Z}_n$) wynosi n.

Dowód:

Niech $\alpha \in \mathbb{Z}/(n)$, $\alpha = [a]$ dla pewnego $a \in \mathbb{Z}$.
Podzielmy a przez n z resztą ($n \neq 0$): $a = bn + r$, gdzie $b, r \in \mathbb{Z}$, $0 \leqslant r < n$.
Mamy $[a] = [bn + r] = [bn] + [r] = [0] + [r] = [0 + r] = [r]$ ($bn \in (n)$, więc $[bn] = [0]$.
Zatem $\mathbb{Z}/(n) = \{[0], [1], ..., [n-1]\}$.
Niech $k, l \in \mathbb{Z}$, $0 \leqslant k < l \leqslant n - 1$. Jest jasne, że $n \nmid l - k$ tzn. $(l - k) \notin (n)$, więc $l \not\equiv k$, tzn. $[l] = [k]$. Ostatecznie $|\mathbb{Z}/(n)| = n$.

Uwaga:

Niech $p \in \mathbb{P}$, $f \in \mathbb{Z}_p[X]$, $deg(f) = d$, $f \neq 0$. Podobnie pokazujemy, że $|\mathbb{Z}_p[X]/(f)| = p^d$, przy czym $\mathbb{Z}_p[X]/(f) = \{[g] : g \in \mathbb{Z}_p[X], deg(g) < d\}$, ($[h] = [qf + r] = [r]$, $deg(r) < deg(f) = d$, $h \in \mathbb{Z}_p[X]$).

Stwierdzenie 5.3

Niech $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Wtedy $[a] \in \mathbb{Z}_n^* \Leftrightarrow NWD(a, n) = 1$.

Dowód:

"$\Rightarrow$"
Przypuśćmy, że $[a] \in \mathbb{Z}_n^*$ tzn. że $[a][b] = 1$ dla pewnego $b \in \mathbb{Z}$.
Zatem $[ab] = 1$ tzn. $ab \equiv 1(n)$ tzn. $n | ab - 1$. Niech $d \in \mathbb{N}$, $d|a$, $d|n$. Wtedy $d|1$ ($d|n|ab - 1$, $d|a \Rightarrow d|ab - 1 + ab$). Zatem $NWD(a, n) = 1$.

"$\Leftarrow$"
Przypuśćmy, że $NWD(a, n) = 1$. Wtedy $xa + yn = 1$ dla pewnych $x, y \in \mathbb{Z}$.
$[xa + yn] = [1]$
$[x][a] = [1]$, co oznacza, że $[a] \in \mathbb{Z}_n^*$ ($[a]^{-1} = [x]$.

Uwaga:
Podobnie pokazujemy (przykładowo), że jeśli $p \in \mathbb{P}$, $f, g \in \mathbb{Z}_p[X]$, $f \neq 0$, to $[g] \in (\mathbb{Z}_p[X]/(p))^* \Leftrightarrow NWD(g, f) \sim 1$. To kryterium na odwracalność działa w dowolnej DIG.

Dążymy do sformułowania (algebraicznej wersji) chińskiego twierdzenia o resztach (CRT). Potrzebne nam pojęcie izomorfizmu pierścieni.

Przykład (motywujący):
$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ - ciało
Niech $A_1 = \mathbb{Z}_7[x]/(x^2 - 5)$, $A_2 = \mathbb{Z}_7[x]/(x^2 - 6)$.
Zauważmy, że A_1 i A_2 to ciała (7^2 elementów) co wynika z:

Stwierdzenie 5.4

Niech D będzie DIG, $a \in D$, $a \neq 0$, $a \notin D^*$. Wówczas:

1. Jeśli a jest nierozkładalny, to $D/(a)$ jest ciałem.
2. Jeśli a jest rozkładalny, to $D/(a)$ nie jest dziedziną całkowitości, więc tym bardziej nie jest ciałem.

(przykład i dowód stwierdzenia do dokończenia na kolejnym wykładzie)
Dowód:

1. Załóżmy, że a jest nierozkładalny.
   Niech $\beta \in D/(a), \beta = [b]$ (klasa pewnego elementu $b \in D$)
   Skoro D jest DIG to $(a, b) = (c)$ dla pewnego $c \in D$.
   $c|a$ ponieważ $(a) \subset (a, b) = (c)$ więc $a \in (c)$
   Ale a jest nierozkładalny, czyli $c \sim a \vee c \in D^*$

   - Przypuśćmy, że $c \in D^*$.
     Wtedy $(c) = D$, w szczególności $1 \in (c) = (a, b)$
     Stąd $1 = xa + yb$ dla pewnych $x, y \in D$
     Mamy $[1] = [x][a] + [y][b]$, $[a] = [0]$ w $D/(a)$
     Zatem $[1] = [y][b]$
     $[b] = \beta$ jest odwracalne w $D/(a)$
   - Załóżmy, że $c \sim a$
     Wtedy $(a, b) = (c) = (a)$
     Otrzymujemy, że $a|b$ bo $b \in (a, b) = (a)$
     to znaczy, że $b = da$ dla pewnego $d \in D$
     Stąd $\beta = [b] = [d][a] = [0]$

   Pokazaliśmy, że jeśli a jest nierozkładalne to albo β jest odwracalne albo $\beta = [0]$
2. Jeśli a jest rozkładalny czyli $a = a_1 a_2$ gdzie $a_1, a_2 \in D/D^*$
   $[0] = [a] = [a_1][a_2]$
   Pozostaje zauważyć, że $[a_1], [a_2] \neq [0]$
   Przymuśćmy, że $[a_1] = [0]$
   To oznacza, że $a_1 \equiv 0 (mod\ a)$
   $a_1 - 0 = a_1 \in (a)$
   Innymi słowy $1|a_1$ czyli $a_1 = da$ dla $d \in D$
   $a = a_1 a_2 = daa_2$
   Skoro D jest dziedziną to możemy skrócić przez $a \neq 0$
   $1 = da_2 \Rightarrow a_2$ jest odwracalny, co prowadzi do sprzeczności: $a_2 \in D^*$
   Zatem $[a_1] \neq [0]$
   Analogicznie dowodzimy $[a_2] \neq [0]$

6

Z tego stwierdzenia wynika następujący przykład:

Przykład 6.1

Zadanie 1. Pokaż, że pierścienie ilorazowe $A_1 = \mathbb{Z}_7[x]/(x^2-5)$ oraz $A_2 = \mathbb{Z}_7[x]/(x^2-6)$ są tymi samymi ciałami.

Rozwiązanie Zadania 1.
Z wspomnianego stwierdzenia wiemy, że oba są ciałami. Wiemy też, że mają po 7^2 elementów.
Uzasadnijmy, że są tym samym ciałem z dokładnością do nazwy elementów (bez powoływania się na teorię ciał skończonych).
Przyjrzyjmy się najpierw 7^2 elementowemu ciału $\mathbb{Z}_7[x]/(x^2-5)$
Mamy w nim $[x^2-5] = [0]$, więc $[x^2] = [5]$
Innymi słowy $[x]$ jest pierwiastkiem kwadratowym z $[5]$ w $\mathbb{Z}_7[x]/(x^2-5)$
Zamiast $[5]$ możemy pisać po prostu 5, bo $\mathbb{Z}_7[x]/(x^2-5)$ zawiera kopię ciała $\mathbb{Z}_7$.
Formalnie: $\mathbb{Z}_7 \ni a \mapsto [a] \in \mathbb{Z}_7[x]/(x^2-5)$
W takiej sytuacji piszemy $[x] = \sqrt{5}$
$\mathbb{Z}_7[x]/(x^2-5) = \mathbb{Z}_7(\sqrt{5})$ (ciało $\mathbb{Z}_7[x]$ poszerzone o $\sqrt{5}$).
Podobnie $\mathbb{Z}_7[x]/(x^2-6) = \mathbb{Z}_7(\sqrt{6}), [x] = [6]$
W $\mathbb{Z}_7[x]/(x^2-5)$:

$\sqrt{5}$ jest oznaczony $[x]_{x^2-5}$

$\sqrt{6} = 2\sqrt{5}$, bo $(2\sqrt{5})^2 = 6(mod\ 7)$ jest oznaczony $[2x]_{x^2-5}$

W $\mathbb{Z}_7[x]/(x^2-6)$:

$\sqrt{6}$ jest oznaczony $[x]_{x^2-6}$

$\sqrt{5} = 4\sqrt{6}$, bo $(4\sqrt{6})^2 = 5(mod\ 7)$ jest oznaczony $[4x]_{x^2-6}$

Innymi słowy $\mathbb{Z}_7[x]/(x^2-5)$ i $\mathbb{Z}_7[x]/(x^2-6)$ jest tym samym ciałem z dkoładnością do nazwania elementów. Działania są takie same (mod 7).

Definicja 6.1: Izomorfizm

Niech R_1, R_2 będą pierścieniami przemiennymi z 1. IZOMORFIZMEM R_1 na R_2 nazywamy bijekcję $f : R_1 \to R_2$ taką, że:
$f(a+b) = f(a) + f(b)$
$f(ab) = f(a)f(b)$
$f(1_{R_1}) = 1_{R_2}$
dla dowolnych $a, b \in R_1$
Do otrzymania definicji MONOMORFIZMU, EPIMORFIZMU i HOMOMORFIZMU trzeba zamienić w definicji izomorfizmu słowo "bijekcja" na odpowiednio "injekcja", "surjekcja" i "funkcja".

Pokażemy formalnie, że $\mathbb{Z}_7[x]/(x^2-5) \simeq \mathbb{Z}_7[x]/(x^2-6)$ (są izomorficzne).
Przydadzą się stwierdzenia:

Stwierdzenie 6.1

Niech R_1, R_2 - pierścienie przemienne z 1. $f : R_1 \to R_2$ jest homomorfizmem.
Wówczas: $ker\ f = f^{-1}(\{0\}) \lhd R_1$ (jest ideałem R_1)

Stwierdzenie 6.2

Homomorfizm f pierścieni przemiennych z 1 jest monomorfizmem wtedy i tylko wtedy gdy $kerf = \{0\}$

Dowód:
Dla $a \in R_1$: $g([a]) = 0 \Leftrightarrow f(a) = 0 \Leftrightarrow a \in kerf \Leftrightarrow [a] = [0]$

Stwierdzenie 6.3: Twierdzenie o izomorfizmie

Niech R_1, R_2 - pierścienie przemienne z 1. $f : R_1 \to R_2$ jest epimorfizmem.
Wtedy istnieje dokładnie jeden izomorfizm g, taki, że poniższy diagram jest przemienny.

$$\begin{tikzcd} R_1 \arrow[r, "f"] \arrow[d, "\prod"] & R_2 \\ R_1/ker\ f \arrow[ur, "g"] & \end{tikzcd}$$

gdzie $\prod$ to rzutowanie kanoniczne, $\prod(a) = a + ker\ f$

Dowód:
$g : R_1/ker\ f \to R_2$ musi być określone wzorem $g([a]) = f(a)$

(i) g jest dobrze określone: załóżmy, że $a, b \in R_1, [a] = [b]$.
To oznacza, że $a - b \in ker\ f$.
Stąd $f(a - b) = f(0) = 0$.
To znaczy: $f(a) - f(b) = 0, f(a) = f(b)$, czyli:
$g([a]) = g([b])$

(ii) g jest homomorfizmem.
Dla $a, b \in R_1$ mamy $g([a][b]) = g([ab]) = f(ab) = f(a)f(b) = g([a])g([b])$
Podobnie dla dodawania.
Wreszcie $g([1]) = f(1) = 1$

(iii) g jest izomorfizmem.
g jest "na" bo f jest "na".
g jest monomorfizmem bo $kerg = [0]$.

Pokażemy teraz $\mathbb{Z}_7[x]/(x^2 - 5) \simeq \mathbb{Z}_7[x]/(x^2 - 6)$
Niech $f : \mathbb{Z}_7[x] \mapsto \mathbb{Z}_7[x]/(x^2 - 6)$
$x \mapsto [4x]$, tak by $ker\ f = (x^2 - 5)$
f jest homomorfizmem, f jest "na".
Z twierdzenia o izomorfiźmie $\mathbb{Z}_7[x]/(x^2 - 6) \simeq \mathbb{Z}_7[x]/ker\ f$
Mamy $ker\ f = (x^2 - 5)$
$(x^2 - 5) \mapsto [4x]^2 - [5] = [0]$
Niech $w \in \mathbb{Z}_7[x], f(w) = [0]$
$w = (x^2 - 5)Q + R, def\ R < 2$
$[0] = f(w) = f(x^2 - 5)f(Q) + f(R) = [0]f(Q) + f(R) = f(R)$
Czyli: $f(R) = [0]$
Jako, że R jest postaci: $R = ax + b$
$[0] = f(R) = f(ax) + f(b) = [4ax] + [b]$
Stąd: $a = b = 0$
$x^2 - 6|4ax + b$ oraz $ax + b = 0$

7

Twierdzenie 7.1: Chińskie Twierdzenie o Resztach (CRT) dla $\mathbb{Z}$

Niech $n = n_1 \cdot ... \cdot n_k$, gdzie $n_i \in \mathbb{N}$, $NWD(n_i, n_j) = 1$ dla $i \neq j$.
Wówczas $\mathbb{Z}_n = \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$.

Dowód:
Niech $f : \mathbb{Z} \longrightarrow \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$.
$a \mapsto (a \pmod{n_1}, ..., a \pmod{n_k})$
f jest homomorfizmem (bo każda $a \mapsto a \pmod{n_i}$ jest homomorfizmem)
$ker(f) = \{a \in \mathbb{Z} : a \in (n_1), ..., a \in (n_k)\} = (n_1) \cap ... \cap (n_k) = (NWW(n_1, ..., n_k)) =$
$= (n_1 \cdot ... \cdot n_k) = (n)$, bo $NWD(n_i, n_j) = 1$ dla $i \neq j$.
Z twierdzenia o izomorfizmie (6.3) $\mathbb{Z}_n = \mathbb{Z}/(n) \simeq im(f)$.
W szczególności $|\mathbb{Z}_n| = |im(f)| \leqslant |\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}|$.
Skoro $|\mathbb{Z}_n| = n = n_1 \cdot ... \cdot n_k = |\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}|$, to $im(f) = \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$.

Metoda 7.1

W praktyce chcemy rozwiązać układ kongruencji

$$\begin{cases} a \equiv b_1 \pmod{n_1} \\ \vdots \\ a \equiv b_k \pmod{n_k} \end{cases}$$

dla pewnych $b_1, ..., b_k \in \mathbb{Z}$. Szukamy $a \in \mathbb{Z}$ spełniającego ten układ.

Niech $N_i = \frac{n}{n_i} = \prod_{j \neq i, 1 \leqslant j \leqslant k} n_j$.
$NWD(N_i, n_i) = 1$ (bo $NWD(n_i, n_j) = 1$ dla $i \neq j$)
Istnieją więc $x, y \in \mathbb{Z}$ (które można znaleźć za pomocą algorytmu Euklidesa) takie, że $x_i N_i + y_i n_i = 1$. Weźmy $a = x_1 N_1 b_1 + ... + x_k N_k b_k$.
$a \equiv b_i \pmod{n_i}$ - składnik $x_i N_i b_i \equiv b_i \pmod{n_i}$, a pozostałe $\equiv 0 \pmod{n_i}$, bo $n_i | N_l$ dla $l \neq i$.

Ogólnie CRT zachodzi w dowolnym pierścieniu przemiennym z 1.

Twierdzenie 7.2

Niech R - pierścieniem przemiennym z 1, $I_1, ..., I_k$ - ideały pierścienia R, $I_s + I_t = R$ dla $s \neq t$.
Wówczas $R/(I_1 \cap ... \cap I_k) \simeq R/I_1 \times ... \times R/I_k$.

Wniosek 7.1

Przy oznaczeniach z twierdzenia 7.1
$\mathbb{Z}_n^* \simeq \mathbb{Z}_{n_1}^* \times ... \times \mathbb{Z}_{n_k}^*$.

Dowód:
Izomorfizm grup jest obcięciem izomorfizmu pierścienia:
$g : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$
Wynika to z ogólnego faktu: Jeśli $g : R_1 \to R_2$ jest izomorfizmem pierścieni przemiennych z 1, to $g|_{R^*}$ jest izomorfizmem grup $R_1^* \to R_2^*$, ponieważ mamy $g(R_1^*) \subset R_2^*$.
Wyjaśnimy teraz dlaczego $g(R_1^*) \subset R_2^*$. Jeśli $r \in R_1^*$, to $rs = 1$ dla pewnego $s \in R_1^*$. Stąd $g(r)g(s) = g(rs) = g(1) = 1$, zatem $g(r) \in R_2^*$.
Stosując to samo rozumowanie dla g^{-1}, mamy $g^{-1}(R_2^*) \subset R_1^*$, więc $R_2^* = gg^{-1}(R_2^*) \subset g(R_1^*)$.

Definicja 7.1: funkcja ϕ Eulera

Dla $n \in \mathbb{N}$ określamy FUNKCJĘ EULERA jako $\phi(n) = |\mathbb{Z}_n^*|$.

Uwaga:
Zauważmy (ze stwierdzeń 5.2 i 5.3), że $\phi(n) = |\{m \in \mathbb{N} : 1 \leqslant m \leqslant n, NWD(m,n) = 1\}|$.

Wniosek 7.2

Niech $n_1, n_2 \in \mathbb{N}, NWD(n_1, n_2) = 1$. Wtedy $\phi(n_1 n_2) = \phi(n_1)\phi(n_2)$,
tzn. funkcja ϕ jest multiplikatywna.

Dowód:
$\phi(n_1 n_2) = |\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*| = |Z_{n_1}^*| \cdot |Z_{n_2}^*| = \phi(n_1)\phi(n_2)$

Motywacja:
Szukamy "wzoru" na $\phi(n)$.
Niech $n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$. Wtedy z wniosku 7.2 $\phi(n) = \prod_{p \in \mathbb{P}} \phi(p^{\alpha_p})$.
Pozostaje znaleźć wzór na $\phi(p^\alpha)$ dla $p \in \mathbb{P}$, $\alpha \in \mathbb{N}$.

Stwierdzenie 7.1

Dla $p \in \mathbb{P}, \alpha \in \mathbb{N}$ mamy $\phi(p^\alpha) = p^{\alpha-1}(p-1)$.

Dowód:
$\phi(p^\alpha) = |\{m \in \mathbb{N} : 1 \leqslant m \leqslant p^\alpha, NWD(m, p^\alpha) = 1\}| =$
$= p^\alpha - |\{m \in \mathbb{N} : 1 \leqslant m \leqslant p^\alpha, NWD(m, p^\alpha) > 1\}| =$
$= p^\alpha - |\{m \in \mathbb{N} : 1 \leqslant m \leqslant p^\alpha, p|m\}| =$
$= p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

Wniosek 7.3

Niech $n \in \mathbb{N}, n = \prod\limits_{p \in \mathbb{P}} p^{\alpha_p}$. Wtedy $\prod\limits_{p \in \mathbb{P}} p^{\alpha_p - 1}(p-1) = n \prod\limits_{p \in \mathbb{P}} (1 - \frac{1}{p})$

Kryptosystem RSA:
Bob chce wysłać Alicji zaszyfrowaną wiadomość, którą tylko ona będzie mogła odszyfrować. Alicja wcześniej wygenerowała swój klucz publiczny (n, e) w następujący sposób:

- Alicja wybiera dwie różne "duże" liczby pierwsze p, q.
- Oblicza $n = pq$.
- Wybiera tzw. wykładnik szyfrujący $e \in \mathbb{N}$, $1 \leqslant e \leqslant \phi(n)$, $NWD(e, \phi(n)) = 1$.
- Oblicza tzw. wykładnik deszyfrujący $d \in \mathbb{N}$, $1 \leqslant d \leqslant \phi(n)$, $ed \equiv 1 \pmod{\phi(n)}$ (za pomocą rozszerzonego algorytmu Euklidesa).
- Ujawnia klucz publiczny (n, e).
- Chroni swój klucz prywatny d.

Wiadomością jawną Boba jest $m \in \mathbb{Z}_n$. Bob wysyła Alicji szyfrogram $m =: c$. Alicja odczytuje m, obliczając $c^d = (m^e)^d = m^{ed} = m$. Równość $m^{ed} = m$ dla $m \in \mathbb{Z}_n^*$ wynika z twierdzenia Eulera:

Twierdzenie 7.3: Euler

Niech $n \in \mathbb{N}, a \in \mathbb{Z}_n^*$. Wtedy $a^{\phi(n)} = 1$.

Dowód:
Twierdzenie wynika z twierdzenia Lagrange'a w grupie Z_n^* mocy $\phi(n)$.

Uwaga:
$ed \equiv 1 \pmod{\phi(n)}$ oznacza, że $ed = 1 + k\phi(n)$. Dla $m \in \mathbb{Z}_n^*$ mamy $m^{ed} = m(m^{\phi(n)})^k = = m \cdot 1^k = m$.
ćwiczenie - pokazać, że założenie $m \in \mathbb{Z}_n^*$ jest zbędne w $m^{ed} = m$.

8 Twierdzenie Czebyszewa

Rozszerzając wiedze z poprzedniego wykładu, będziemy się zastanawiać nad następującym pytaniem. Jak generować *duże* liczby pierwsze w przedziale $(n, kn]$ dla pewnej stałej $k > 1$ i *dużego* $n \in \mathbb{N}$. Służyć nam będzie do tego twierdzenie Czebyszewa do którego będziemy dochodzić w tym rozdziale. do jego dowodu będziemy potrzebowali kilku lematów.

Lemat 8.1

Niech $n \in \mathbb{N}$. Wtedy

$$N := \text{NWW}(n+1, n+2, ..., 2n+1) \geqslant 4^n$$

Dowód:
Rozważmy

$$I = \int_0^1 (x(1-x))^n \, dx$$

Zauważmy, że $0 \leqslant x(1-x) \leqslant \frac{1}{4}$ na przedziale $[0, 1]$. Stąd:

$$0 \leqslant (x(1-x))^n \leqslant 4^{-n}$$

$$0 \leqslant I \leqslant 4^{-n}$$

Mamy

$$x^n(1-x)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i x^{n+i}$$

$$\int_0^1 x^n(1-x)^n \, dx = \sum_{i=0}^{n} \binom{n}{i} (-1)^i \frac{1}{n+i+1}$$

Zatem $N \cdot I \in \mathbb{N}$

$$N \cdot I \geqslant 1$$

$$N \geqslant I^{-1} > 4^n$$

Lemat 8.2

Niech $x \geqslant 1$. Wtedy

$$\prod_{\substack{p \leqslant x \\ p \in \mathbb{P}}} p \leqslant 4^x$$

Dowód:
Zauważmy, że jeśli udowodnimy lemat dla $x \in \mathbb{N}$, to

$$\prod_{\substack{p \leqslant x \\ p \in \mathbb{P}}} p = \prod_{\substack{p \leqslant \lfloor x \rfloor \\ p \in \mathbb{P}}} p \leqslant 4^{\lfloor x \rfloor} \leqslant 4^x$$

Niech więc $x \in \mathbb{N}, x = n$. Przeprowadźmy indukcję ze względu na n:

- dla $n = 1$
$$\prod_{\substack{p \leqslant x \\ p \in \mathbb{P}}} p = 1 < 4^1$$
- niech $n \in \mathbb{N}$, $n > 1$. Załóżmy, że $\prod_{\substack{p \leqslant m \\ p \in \mathbb{P}}} p \leqslant 4^m$ dla $n \in \mathbb{N}, m \leqslant n$.
  - Jeśli n - nieparzysta, to
  $$\prod_{\substack{p \leqslant n+1 \\ p \in \mathbb{P}}} p = \prod_{\substack{p \leqslant n \\ p \in \mathbb{P}}} p \leqslant 4^n < 4^{n+1}$$
  - Załóżmy teraz, że n jest parzysta $n = 2k$. Mamy
  $$\prod_{\substack{p \leqslant 2k+1 \\ p \in \mathbb{P}}} p = \prod_{\substack{p \leqslant k+1 \\ p \in \mathbb{P}}} p \cdot \prod_{\substack{k+1 < p < 2k+1 \\ p \in \mathbb{P}}} p$$

Ponadto zauważmy, że

$$\prod_{\substack{k+1<p\leqslant 2k+1\\ p\in\mathbb{P}}} p \,\Big|\, \frac{(2k+1)!}{(k+1)!k!} = \binom{2k+1}{k+1}$$

Ponieważ dzieli licznik, a nie dzieli mianownik.

Skoro więc $2^{2k+1} = (1+1)^{2k+1} = \binom{2k+1}{k} + \binom{2k+1}{k+1} = 2\cdot\binom{2k+1}{k+1}$ to

$$\prod_{\substack{k+1<p\leqslant 2k+1\\ p\in\mathbb{P}}} p \leqslant \frac{1}{2}2^{2k+1} = 2^{2k}$$

Ostatecznie otrzymujemy

$$\prod_{\substack{k+1<p\leqslant 2k+1\\ p\in\mathbb{P}}} p \leqslant 4^{k+1}\cdot 4^k = 4^{2k+1}$$

Uzbrojeni w te lematy, możemy przejść do finałowego twierdzenia tego wykładu:

Twierdzenie 8.1: Czebyszewa

Istnieją stałe dodatnie a i b (na przykład $a = \frac{\ln 2}{2}, b = \frac{2}{e} + 4\ln 2$) takie że

$$a\cdot\frac{x}{\ln x} < \Pi(x) < b\cdot\frac{x}{\ln x}, \qquad x \geqslant 2$$

Dowód:
Niech $n\in\mathbb{N}$ będzie takie, że $2n+1 \leqslant x \leqslant 2n+3$. Mamy

$$\mathrm{NWW}(n+1,...,2n+1) = \prod_{p\in\mathbb{P}} p^{\max\{v_p(n+1),...,v_p(2n+1)\}}$$

gdzie $v_p(m) = \max\left\{l\in\mathbb{Z}_{\geqslant 0} : p^l|m\right\}$ Przy tym zauważmy, że

$$\max\{v_p(n+1),...,v_p(2n+1)\} = \max\{\alpha_p\in\mathbb{Z} : p^{\alpha_n} \geqslant 2n+1\} := \beta_p$$

Stąd

$$N = \prod_{p\in\mathbb{P}} p^{\beta_n} \leqslant (2n+1)^{(2n+1)}$$

Z lematu 8.1 otrzymujemy, że $(2n+1)^{(2n+1)} > 4^n$. Stąd

$$(2n+1) > \frac{n\ln 4}{\ln(2n+1)}$$

Ostatecznie $\prod(x) \geqslant \prod(2n+1) > \frac{n\ln 4}{\ln(2n+1)}$. Dodatkowo $n > \frac{x-3}{2}$ oraz $\ln(2n+1) \leqslant \ln(x)$ więc

$$\Pi(x) > \frac{(x-3)\ln 4}{2\ln x} \geqslant \frac{x\ln 2}{2\ln x}$$

Bo dla $x\geqslant 6$ zachodzi $2(x-3)\geqslant x$,a dla $x\leqslant 5$ można bezpośrednio pokazać, że

$$\Pi(x) > \frac{\ln 2}{2}\cdot\frac{x}{\ln x}$$

Co kończy dowód.

Wniosek 8.1

Niech $k > \frac{b}{a}$, stała c taka że $0 < c < ak - b$. Wówczas

$$\Pi(kn) - \Pi(n) > c\cdot\frac{\ln n}{n}, \qquad n \geqslant n_0$$

Dowód:
Z tw. Czebyszewa mamy

$$\prod(kn) - \prod(n) > \frac{akn}{\ln kn} - \frac{bn}{\ln n} = \frac{n}{\ln n}\left(\frac{ak\ln n}{\ln kn} - b\right)$$

Chcemy, by

$$\frac{ak\ln n}{\ln kn} - b > c$$
$$ak\ln n > (b+n)\ln(kn)$$
$$ak\ln n - (b+n)\ln n > (b+c)\ln k$$
$$\ln n > \frac{(b+c)\ln k}{ak-b-c}$$
$$n \geqslant \exp\left(\frac{(b+c)\ln k}{ak-b-c}\right)$$

co kończy dowód

Wniosek 8.2

Przy oznaczeniach z Wniosku 8.1, to oczekiwana liczba losowań liczby $n \in \mathbb{N}, m \in (n, kn]$ aż do otrzymania $m \in \mathbb{P}$ jest równa co najwyżej $\frac{k-1}{c}\ln n$

Dowód:
Ta liczba to zmienna losowa X, gdzie

$$\mathbb{P}(X = i) = (i-t)^{i-1}\cdot t \qquad t = \frac{\prod(kn) - \prod(n)}{\lfloor kn - n\rfloor}$$

Jest to rozkład geometryczny z parametrem t, więc jego wartośc oczekiwana wynosi

$$\mathbb{E}X = \frac{1}{t}\cdot\frac{\lfloor kn-n\rfloor}{\prod(kn) - \prod(n)}$$

Z Wniosku 8.1

$$\mathbb{E}X < \frac{n(k-1)\cdot\ln n}{cn} = \frac{k-1}{c}\cdot\ln n$$

co kończy dowód.

9

Do sformułowania pierwszego testu pierwszości (a raczej złożoności), testu Solovaya-Strassena, potrzebny jest symbol Legendre'a oraz jego uogólnienie -symbol Jacobiego

Definicja 9.1: symbol Legendre'a

Niech $p \in \mathbb{P} \backslash \{2\}$, $QR(p) = \{b^2 : b \in \mathbb{Z}_p^*\}$ — reszty kwadratowe, $QN(p) = \mathbb{Z}_p^* \backslash QR\{p\}$ — niereszty kwadratowe.

Dla $a \in \mathbb{Z}$ definiujemy $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ jeśli } p|a \\ 1 \text{ jeśli } a \pmod p \in QR(p) \\ -1 \text{ jeśli } a \pmod p \in NQ(p) \end{cases}$

i nazywamy SYMBOLEM LEGENDRE'A

Twierdzenie 9.1: własności symbolu Legendre'a

Niech $p \in \mathbb{P} \backslash \{2\}$, $a, b \in \mathbb{Z}$. Wówczas zachodzą własności:

1. $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ (wzór Eulera)
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ jeśli } p \equiv 1 \pmod 4 \\ -1 \text{ jeśli } p \equiv 3 \pmod 4 \end{cases}$
5. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \text{ jeśli } p \equiv \pm 1 \pmod 8 \\ -1 \text{ jeśli } p \equiv \pm 3 \pmod 8 \end{cases}$
6. $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{p}{q}\right) \text{ jeśli } p \equiv q \equiv 3 \pmod 4 \\ \left(\frac{p}{q}\right) \text{ w p.p.} \end{cases}$

Dowód:

1. Wynika wprost z definicji.
2.
   - Jeśli $p|a$, to $(\frac{a}{p}) = 0$ i $a^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} \equiv 0$
   - Załóżmy, że $a \pmod p \in QR(p)$, tzn. że $a \pmod p = b^2$ dla pewnego $b \in \mathbb{Z}_p^*$.
     Wtedy $a^{\frac{p-1}{2}} \pmod p = (b^2)^{\frac{p-1}{2}} = b^{p-1} = 1$ (z małego tw. Fermata).
     Z definicji $(\frac{a}{p}) = 1$.
   - Załóżmy, że $a \pmod p \in QN(p)$. Niech $\mathbb{Z}_p^*$ będzie generowana przez g.
     Mamy $a \pmod p = g^k$ dla pewnego $k \in \mathbb{N}, 2 \nmid k$.
     $a^{\frac{p-1}{2}} \pmod p = (g^k)^{\frac{p-1}{2}}) = (g^{\frac{p-1}{2}})^k = (-1)^k = -1$. Z definicji $(\frac{a}{p}) = -1$.
3. $(\frac{ab}{p}) \equiv_p (ab)^{\frac{p-1}{2}} \equiv_p a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv_p (\frac{a}{p})(\frac{b}{p})$. Otrzymujemy de facto równość $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
4. Ze wzoru Eulera: $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Znów jest to tak naprawdę równość.
5. Rozważmy $N_p = |\{(x, y) \in \mathbb{Z}_p^2 : x^2 + y^2 = 2\}|$. Najpierw "obliczmy" $N_p \pmod 8$.
   $N_p = \underbrace{|\{y \in \mathbb{Z}_p : y^2 = 2\}|}_{\text{pary (0,y)}} + \underbrace{|\{x \in \mathbb{Z}_p : x^2 = 2\}|}_{\text{pary (x,0)}} + \underbrace{|\{x \in \mathbb{Z}_p : x^2 = 1\}|}_{\text{pary (x,x)}} + \underbrace{|\{x \in \mathbb{Z}_p : x^2 = 1\}|}_{\text{pary (x,-x)}} +$
   $8k$ dla pewnego $k \in \mathbb{N}$.
   Użyjemy teraz następującego lematu:

   Lemat 9.1

   Niech $p \in \mathbb{P} \backslash \{2\}, a \in \mathbb{Z}_p$. Wówczas $|\{x \in \mathbb{Z}_p : x^2 = a\}| = 1 + \left(\frac{a}{p}\right)$.

Dowód lematu:

$$1 + (\tfrac{a}{p}) = \begin{cases} 1 + 0 = 1 \text{ jeśli } a = 0 \\ 1 + 1 = 2 \text{ jeśli } a \in QR(p) \\ 1 - 1 = 0 \text{ jeśli } a \in QN(p) \end{cases}$$

Wracając do dowodu 5. mamy więc $N_p \equiv_8 2(a + (\frac{2}{p})) + 4 \equiv_8 6 + 2\left(\frac{p}{2}\right)$.

10

Ciąg dalszy dowodu:

5.

Lemat 10.1

- Dla $p \in \mathbb{P} \backslash \{2\}$ mamy $|QR(p)| = \frac{p-1}{2} = |QN(p)|$

Dowód:
Niech $f : \mathbb{Z}_p^* \mapsto QR(p)$, f jest epimorfizmem.
$ker f = \{x \in \mathbb{Z}_p^* : x^2 = 1\} = \{-1, 1\}$
Z twierdzenia o izomorfiźmie:
$QR(p) \simeq \mathbb{Z}_p^* / \{-1, 1\}$
W szczególności ma moc $\frac{p-1}{2}$
$|QN(p)| = |\mathbb{Z}_p^*| - |QR(p)| = \frac{p-1}{2}$

Wniosek 10.1: Z lematu

Dla $p \in \mathbb{P} \backslash \{2\}$ mamy $\sum\limits_{a \in \mathbb{Z}_p} \left(\frac{a}{p}\right) = 0$

Dowód:
$$\sum_{a \in \mathbb{Z}_p} \left(\frac{a}{p}\right) = \left(\frac{0}{p}\right) + \sum_{a \in QR(p)} \left(\frac{a}{p}\right) + \sum_{a \in QN(p)} \left(\frac{a}{p}\right) = 0 + \frac{p-1}{2} \cdot 1 + \frac{p-1}{2} \cdot (-1) = 0$$

Lemat 10.2

Dla $p \in \mathbb{P} \backslash \{2\}$, $a \in \mathbb{Z}_p^*$, $B = \{(x, y) \in \mathbb{Z}_p^2 : x^2 + y^2 = a\}$ mamy:
$|B| = p - \left(\frac{-1}{p}\right)$

Dowód:
$$|B| = \sum_{t_1, t_2 \in \mathbb{Z}_p, t_1 + t_2 = a} |\{x \in \mathbb{Z}_p : x^2 = t_1\}||\{y \in \mathbb{Z}_p : y^2 = t_2\}|$$
Z lematu 9.1:
$|B| =$
$$= \sum_{t_1, t_2 \in \mathbb{Z}_p, t_1 + t_2 = a} (1 + \left(\frac{t_1}{p}\right))(1 + \left(\frac{t_2}{p}\right)) =$$
$$= \sum_{t \in \mathbb{Z}_p} (1 + \left(\frac{t}{p}\right))(1 + \left(\frac{a-t}{p}\right)) =$$
$$= \sum_{t \in \mathbb{Z}_p} 1 + \sum_{t \in \mathbb{Z}_p} \left(\frac{t}{p}\right) + \sum_{t \in \mathbb{Z}_p} \left(\frac{a-t}{p}\right) + \sum_{t \in \mathbb{Z}_p} \left(\frac{t}{p}\right) \left(\frac{a-t}{p}\right)$$
Z wniosku 10.1 wiemy, że druga i trzecia suma to 0. Ponadto:
$$\sum_{t \in \mathbb{Z}_p} \left(\frac{t}{p}\right) \left(\frac{a-t}{p}\right) =$$
$$= \sum_{t \in \mathbb{Z}_p^*} \left(\frac{t}{p}\right) \left(\frac{a-t}{p}\right) =$$
$$= \sum_{t \in \mathbb{Z}_p^*} \left(\frac{t^{-2}}{p}\right) \left(\frac{t}{p}\right) \left(\frac{a-t}{p}\right) =$$
$$= \sum_{t \in \mathbb{Z}_p^*} \left(\frac{t^{-1}t}{p}\right) \left(\frac{t^{-1}(a-t)}{p}\right) =$$
$$= \sum_{t \in \mathbb{Z}_p^*} \left(\frac{at^{-1} - 1}{p}\right) =$$
$$= \sum_{s \in \mathbb{Z}_p} \left(\frac{s}{p}\right) - \left(\frac{-1}{p}\right) = -\left(\frac{-1}{p}\right)$$

Ostatecznie: $|B| = p - \left(\frac{-1}{p}\right)$

Kontynuacja dowodu:
Otrzymujemy dla $a = 2$:
$p - \left(\frac{-1}{p}\right) = |A| \equiv 6 + 2\left(\frac{2}{p}\right) \pmod 8$

- dla $p \equiv 1 \pmod 8$ mamy $p \equiv 1 \pmod 4$
  $1 - 1 \equiv 6 + 2\left(\frac{2}{p}\right) \pmod 8$
  $2\left(\frac{2}{p}\right) \equiv -6 \equiv 2 \pmod 8$
  $\left(\frac{2}{p}\right) \equiv 1 \pmod 8$

- dla $p \equiv 3 \pmod 8$ mamy $p \equiv 3 \pmod 4$
  $3 - (-1) \equiv 6 + 2\left(\frac{2}{p}\right) \pmod 8$
  $2\left(\frac{2}{p}\right) \equiv -2 \pmod 8$
  $\left(\frac{2}{p}\right) \equiv -1 \pmod 8$

- Pozostałe przypadki dowodzimy analogicznie.

6.
Niech $p, q \in \mathbb{P}\backslash\{2\}$. Chcemy pokazać, że:
$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \frac{q}{p}$
Możemy założeć, że $p \neq q$. W przeciwnym przypadku obie strony są równe 0.
Niech n będzie rzędem $p \pmod q$ w $\mathbb{Z}_p^*$.
Mamy $p^n\, equiv 1 \pmod q$, $q | p^n - 1$
Niech F będzie ciałem p^n elementowym (wiemy z ćwiczeń, że takie istnieje). W takim razie w $p^n - 1$ elementowym F^* istnieje element u rzędu q (z cykliczności grupy F^*, de facto udowodnionej na ćwiczeniach).
Niech $S = \sum_{x \in \mathbb{Z}_q} \left(\frac{x}{p}\right) u^x \in F$ (definicja jest poprawna ponieważ dla $k, l \in \mathbb{Z}$ mamy $u^k = u^l \Leftrightarrow u^{k-l} = 1 \Leftrightarrow q | k - l \Leftrightarrow k \equiv l \pmod q$)

Lemat 10.3

- $S^2 = q\left(\frac{-1}{q}\right)$

Dowod:
$S^2 =$
$$= \sum_{x \in \mathbb{Z}_q} \left(\frac{x}{q}\right) u^x \sum_{y \in \mathbb{Z}_q} \left(\frac{y}{q}\right) u^y =$$
$$= \sum_{x,y \in \mathbb{Z}_q} \left(\frac{xy}{q}\right) u^{x+y} =$$
$$= \sum_{t \in \mathbb{Z}_q} \sum_{x,y \in \mathbb{Z}_q} \left(\frac{xy}{q}\right) u^t =$$
$$= \sum_{x,y \in \mathbb{Z}_q, x+y=0} \left(\frac{xy}{q}\right) u^0 + \sum_{t \in \mathbb{Z}_q^*} u^t \sum_{x,y \in \mathbb{Z}_q, x+y=t} \left(\frac{xy}{q}\right)$$
Gdzie:
$$\sum_{x,y \in \mathbb{Z}_q, x+y=0} \left(\frac{xy}{q}\right) =$$
$$= \sum_{x \in \mathbb{Z}_q} \left(\frac{x(-x)}{q}\right) =$$
$$= \left(\frac{-1}{q}\right) \sum_{x \in \mathbb{Z}_q} \frac{x^2}{q} =$$
$$= \left(\frac{-1}{q}\right) \sum_{x \in \mathbb{Z}_q^*} \frac{x^2}{q} =$$
$$= (q-1)\left(\frac{-1}{q}\right)$$

Dla $t \in \mathbb{Z}_q^*$: $\sum_{x,y\in\mathbb{Z}_q, x+y=t} \left(\frac{xy}{q}\right) =$
$= \sum_{x\in\mathbb{Z}_q} \left(\frac{x(t-x)}{q}\right) =$
$= \left(\frac{-1}{q}\right)$
Dowód taki jak dla lematu 10.2.
Stąd:
$S^2 = (q-1)\left(\frac{-1}{q}\right) + \sum_{t\in\mathbb{Z}_q^*} u^t(-\left(\frac{-1}{q}\right))$
$\sum_{t\in\mathbb{Z}_q} u^t = \sum_{t=0}^{q-1} u^t = \frac{u^q-1}{u-1} = 0$
$\Rightarrow \sum_{t\in\mathbb{Z}_q^*} u^t = 0 - u^0 = -1$
$\Rightarrow S^2 =$
$= \left(\frac{-1}{q}\right)(q-1-(\sum_{t\in\mathbb{Z}_q} u^t - u^0)) =$
$= \left(\frac{-1}{q}\right)(q-1-(0-1)) =$
$= q\left(\frac{-1}{q}\right)$
W szczególności $S \neq 0$ więc S jest odwracalne $S \in F$

Lemat 10.4

$S^{p-1} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{q}{p}\right)$

Dowod:
$S^{p-1} = (S^2)^{\frac{p-1}{2}} = (q\left(\frac{-1}{q}\right))^{\frac{p-1}{2}}$ z lematu 10.3.
Z twierdzenia 9.1 otrzymujemy:
$(-1)^{\frac{q-1}{2}\frac{p-1}{2}} \cdot q^{\frac{p-1}{2}} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \cdot \left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)$

Lemat 10.5

$S^{p-1} = \left(\frac{p}{q}\right)$

Dowod:
$S^{p-1} = S^{-1} \cdot S^p$, gdzie:
$S^p =$
$= (\sum_{x\in\mathbb{Z}_q} \left(\frac{x}{q}\right) u^x)^p =$
$= \sum_{x\in\mathbb{Z}_q} \left(\frac{x}{q}\right)^p u^{xp} =$
$= \sum_{x\in\mathbb{Z}_q} \left(\frac{x}{q}\right) u^{xp} =$
$= \left(\frac{p^2}{q}\right) \sum_{x\in\mathbb{Z}_q} \left(\frac{x}{q}\right) u^{xp} =$
$= \left(\frac{p}{q}\right) \sum_{x\in\mathbb{Z}_q} \left(\frac{xp}{q}\right) u^{xp} =$
$= \left(\frac{p}{q}\right) \sum_{y\in\mathbb{Z}_q} \left(\frac{y}{q}\right) u^{y} =$
$= \left(\frac{p}{q}\right) X$
$S^{p-1} = S^{-1}\left(\frac{p}{q}\right) S = \left(\frac{p}{q}\right)$