Geometryczne liczby.
5. Liczby całkowite, szyfrowanie i geometrie nieeuklidesowe
materiały do ćwiczeń

Projekt „Matematyka dla ciekawych świata”
spisał: Michał Korch

4 maja 2020

1 Podzielność

Zacznijmy od krótkich rozważań liczb pierwszych. Przypomnijmy, że liczba jest pierwsza, jeśli ma dokładnie dwa dzielniki.

Zadanie 1

Wykaż, że suma pięciu kolejnych liczb naturalnych nie może być liczbą pierwszą.

Na wykładzie rozmawialiśmy o notacji kongruencji. Mówimy, że $a \equiv b \pmod{m}$, jeśli a i b mają tę samą resztę z dzielenia przez m, lub inaczej jeśli $a - b$ dzieli się przez m.

Zauważmy, że prawdziwe są następujące fakty o kongruencjach. Niech $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$

a) $a + c \equiv b + d \pmod{m}$,

b) $a \cdot c \equiv b \cdot d \pmod{m}$,

c) $a^n \equiv b^n \pmod{m}$.

Zadanie 2

Na wykładzie uzasadniliśmy regułę podzielności dla 3 (suma cyfr) i wyprowadziliśmy dużo bardziej skomplikowaną regułę dla 7 (suma cyfr pomnożonych przez cyklicznie występujące współczynniki). Znajdźcie analogiczną regułę dla podzielności przez 11.

Zadanie 3

Udowodnij, że liczba $3^{105} + 4^{105}$ jest podzielna przez $13, 49, 181$ i 379, ale nie jest podzielna przez 5 i 11.

Wskazówka: Wskazówki do tego zadania znajdziecie na końcu skryptu.

2 Szyfrowanie symetryczne

Przykładem dość prostego szyfrowania symetrycznego (ale potencjalnie możliwego do rozszyfrowania bez posiadania klucza,choć nie w trywialny sposób) szyfrowania jest szyfr Vigenère'a.

Aby skorzystać z tego szyfru wygodnie mieć następującą tablicę:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Rolę liczby k odgrywa tutaj tajny klucz w postaci jakiegoś słowa lub tekstu. Dla przykładu weźmy klucz TAJNE. Chcąc zaszyfrować jakiś tekst, np: SZYFR VIGENEREA, trzeba znaleźć litery w kolumnie odpowiadającej kolejnym literom klucza (w razie czego go zapętlając) i wierszu odpowiadającym odpowiednim literom szyfrowanej wiadomości. W tym wypadku wyjdzie:

LZHSV OIPRRXRNN

Dobierzcie się w pary. I spróbujmy przekazać sobie zaszyfrowaną wiadomość i ją odszyfrować. Każda para najpierw wybiera sobie wspólny klucz.

Zadanie 4

Wybierz wiadomość składającą się z co najmniej 10 znaków i zaszyfruj ją w szyfrze Vigenère'a z ustalonym kluczem. Przekaż zaszyfrowaną wiadomość drugiej osobie z pary.

Zadanie 5

Odszyfruj otrzymaną wiadomość!

3 Szyfrowanie niesymetryczne

Szyfrowanie niesymetryczne polega na tym, że są takie problemy, które bardzo trudno rozwiązać. Każda osoba jest wyposażona w dwa klucze: publiczny i prywatny. Klucz publiczny, który służy do szyfrowania wiadomości, jest powszechnie dostępny, ale szalenie trudno (tysiące lat obliczeń) jest z niego wyliczyć klucz prywatny, który właściciel trzyma w tajemnicy. Tylko mając klucz prywatny da się odszyfrować wiadomość zaszyfrowaną kluczem publicznym.

Szyfrowanie RSA wykorzystuje fakt, że bardzo trudno jest rozłożyć dużą liczbę na czynniki pierwsze. Upraszczając nieco sytuację (za chwilę przeprowadzimy symulację), kluczem publicznym jest pewna liczba n będąca iloczynem dwóch liczb pierwszych p i q, zaś p i q będą kluczem prywatnym. To szyfrowanie w algorytmie szyfrowania i odszyfrowywania wykorzystuje Twierdzenie Eulera $a^{\varphi(n)} \equiv 1 \pmod{n}$, będącym uogólnieniem Małego Twierdzenia Fermata.

Podzielcie się na pary. Następujące trzy zadania przeprowadzą Was przez proces szyfrowania i odszyfrowania wiadomości.

Zadane 6

Najpierw stworzymy klucze prywatny i publiczny. Wybierz dwie różne, pięciocyfrowe (w rzeczywistości używa się duuuużo większych) liczby pierwsze:
p:
q:
(najwygodniej będzie, jeśli dobierzesz tak te liczby, aby $p-1$ ani $q-1$ nie dzieliło się przez 3)
Oblicz $n = pq$:
Teraz potrzebujemy liczby Eulera dla n, czyli $\varphi(n) = (p-1)(q-1)$:
e: 3
znajdź liczbę d, taką, że de dzieli się przez $\varphi(n)$ z resztą 1
Wskazówka: rozważ z jaką resztą dzieli się przez 3, $\varphi(n)$
d:
Liczby n, e to Twój klucz publiczny. Resztę liczb (w szczególności d) zachowaj w tajemnicy (to Twój klucz prywatny)! Przekaż swój klucz publiczny drugiej osobie z pary.

Zadanie 7

Pora zaszyfrować wiadomość. Dostałeś/aś od osoby z pary jej klucz publiczny. Zapisz go sobie:
n:
e:
Wybierz teraz sobie ciąg czterech znaków składających się z liter od A do I, który będziesz chciał/a przekazać drugiej osobie z pary.
Wiadomość do zaszyfrowania:
Przetłumacz tę wiadomość na 4-ro cyfrową liczbę, A=1, B=2, ... I=9.
m:
Policz resztę z dzielenia przez n liczby m^e :
– to jest zaszyfrowana wiadomość – przekaż ją drugiej osobie z pary.
Wskazówka: Możesz użyć `www.wolframalpha.com` *do policzenia tej reszty. Resztę z dzielenia liczy a przez b liczy się tam wpisując a%b.*

Zadanie 8

Dostałeś od osoby z pary zaszyfrowaną wiadomość w postaci liczby
c:
Oblicz resztę z dzielenia przez n (Twoje) liczby c^d :
Wskazówka: Możesz użyć `www.wolframalpha.com` *do policzenia tej reszty. Resztę z dzielenia liczy a przez b liczy się tam wpisując a%b.*

Przetłumacz tę liczbę na 5-cio literowa wiadomość, A=1, B=2, ... I=9. Gotowe!

Zadanie 9

Przypomnij sobie uogólnienie Małego Twierdzenia Fermata, czyli Twierdzenie Eulera, które mówi, że jeśli a i n są względnie pierwsze, to

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

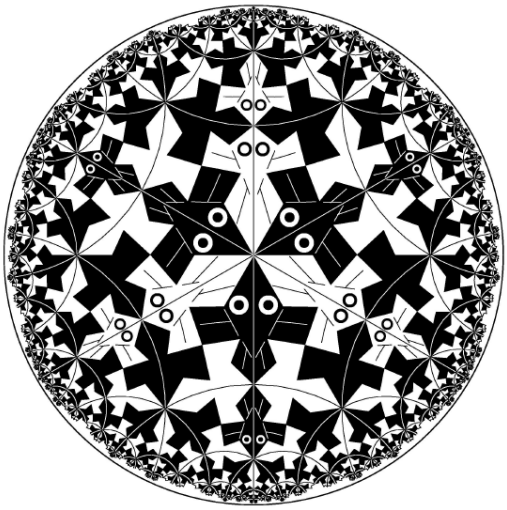
Jak z tego Twierdzenia wynika to, że rzeczywiście otrzymałeś w tym procesie odszyfrowaną wiadomość na końcu?

4 Geometrie nieeuklidesowe

Gdy odrzucimy ostatni (lub nawet nie tylko) ten aksjomat Euklidesa, dostaniemy nowe geometryczne „światy".

Każdy z tych „światów" możemy wyobrazić sobie wewnątrz zwyczajnego euklidesowego świata, nieco zmieniając znaczenie takich słów jak prosta, odległość itp. W skrócie:

1. Geometria euklidesowa:
   - przez punkt poza daną prostą można poprowadzić dokładnie jedną prostą równoległą do niej,
   - suma kątów w każdym trójkącie wynosi 180°.
2. Geometria hiperboliczna:
   - przez punkt poza daną prostą można poprowadzić wiele prostych równoległych do niej,
   - suma kątów w każdym trójkącie jest mniejsza niż 180° i im trójkąt jest większy tym bardziej.
   - modele (należy o nich myśleć, jak o mapach kuli ziemskiej – każda mapa idzie na kompromis i pewne cechy, np. kąty odwzorowuje dobrze, a inne, np. pola źle):
     - Model Poincarégo
       * cała płaszczyzna mieści się w kole bez brzegu,
       * proste to średnice (bez końców) oraz łuki okręgów obustronnie prostopadłych do brzegu (mówimy, że okręgi są prostopadłe, jeśli prostopadłe są proste styczne do nich w tym punkcie)
       * model ten zachowuje kąty, ale oczywiście nie zachowuje odległości i pól (rzeczy się „zagęszczają" im bliżej są brzegu), co dobrze odwzorowuje rysunek Eschera (wszystkie kształty na tym rysunku takie same i takiej samej wielkości (przystające) w tej geometrii)



- Model Kleina
  - cała płaszczyzna, jak wyżej, mieści się w kole bez brzegu,
  - proste to cięciwy tego koła (bez końców),
  - relatywnie łatwo policzyć odległość pomiędzy punktami w tym modelu, używając standardowej linijki. Jeśli chcemy policzyć odległość między punktami A i B prowadzimy prostą (cięciwę) je łączącą. Punkty przecięcia tej cięciwy z okręgiem będącym brzegiem modelu niech będą P i Q, a kolejność punktów na cięciwie to P, A, B, Q. Mierzymy euklidesowe odległości PA, BQ, PB, AQ. Wtedy odległość między A i B w sensie geometrii hiperbolicznej, to:
$$\ln \frac{|PB||AQ|}{|PA||BQ|},$$
gdzie ln to pewna funkcja matematyczna (nosząca nazwę logarytmu naturalnego) – znajdziesz ją na każdym standardowym kalkulatorze,
  - ten model nie zachowuje kątów, ani pól.

3. Geometria sferyczna

   - proste (najkrótsze drogi między punktami) na sferze to wielkie okręgi, czyli okręgi o środku w środku sfery, np. równik i południki, ale już nie równoleżniki,
   - każde dwie proste się przecinają, czyli nie ma prostych równoległych,
   - suma kątów w każdym trójkącie jest większa niż 180°,
   - są takie pary punktów (przeciwległe, zwane też antypodycznymi), przez które można poprowadzić wiele prostych.

4. Geometria eliptyczna (płaszczyzna rzutowa) – model na połówce sfery.

   - Patrzymy na geometrię sferyczną na połówce sfery, z tym że „sklejamy" przeciwległe punkty brzegu tej półsfery. W takim znaczeniu, że jeśli ktoś wyjdzie z jednej strony teleportuje się natychmiast i bez zauważenia tego faktu do przeciwległego punktu.
   - Przez każde dwa punkty w takim razie można poprowadzić dokładnie jedną prostą,
   - Nadal nie ma prostych równoległych, a suma kątów w każdym trójkącie jest większa niż 180°.

Zadanie 10

Na płaszczyźnie euklidesowej narysowano trójkąt. Rozstrzygnij, jaki ma on kształt, jeśli:

a) jeden z jego kątów jest równy sumie dwóch pozostałych?

b) jeden z jego kątów jest mniejszy niż suma dwóch pozostałych?

c) jeden z jego kątów jest większy niż suma dwóch pozostałych?

Wskazówka: Wskazówki do tego zadania znajdziecie na końcu skryptu.

Zadanie 11

A co można powiedzieć o sumie kątów w dowolnym czworokącie (a co o sumie kątów w dowolnym pięciokącie? sześciokącie?) narysowanym w:

a) geometrii euklidesowej?

b) geometrii hiperbolicznej? geometrii na sferze?

Odpowiedzi uzasadnij!

Wskazówka: Wskazówki do tego zadania znajdziecie na końcu skryptu.

Zadanie 12

W geometrii sferycznej poprowadzono trzy proste, które nie przecinają się w jednym punkcie. Na ile i jakich kształtów dzielą one całą sferę?

5 Zadania dodatkowe

Zadanie 13

Która liczba jest większa: 2^{791} czy 5^{339}?

Wskazówka: Wskazówki do tego zadania znajdziecie na końcu skryptu.

Zadanie 14

Udowodnij, że prawdziwe są następujące fakty o kongruencjach. Niech $a \equiv b \pmod{m}$ oraz $c \equiv d \pmod{m}$

a) $a + c \equiv b + d \pmod{m}$

b) $a \cdot c \equiv b \cdot d \pmod{m}$

Zadanie 15

Korzystając z Małego Twierdzenia Fermata udowodnij, że:

a) $2^{20} \equiv 1 \pmod{11}$

b) $9^{221} \equiv 9 \pmod{23}$

Wskazówka: Wskazówki do tego zadania znajdziecie na końcu skryptu.

Zadanie 16

Poszukaj w necie informacji o przeprowadzonym przez A. Wilesa dowodzie Wielkiego Twierdzenie Fermata. Zaznacz działy matematyki były zamieszane w ten dowód?

a) geometria algebraiczna

b) równania różniczkowe

c) analiza zespolona

d) teoria liczb

e) rachunek prawdopodobieństwa

f) topologia

g) algebra abstrakcyjna

h) teoria mnogości

Zadanie 17

Rozstrzygnij, czy na sferze można narysować prostokąt (czworokąt o 4 kątach prostych). A czy istnieje jakikolwiek prostokąt w geometrii hiperbolicznej? Odpowiedzi uzasadnij.

Zadanie 18

Z płaszczyzny rzutowej wycięto koło. Co można powiedzieć o pozostałym fragmencie? Czy da się go sensownie narysować (tak, żeby nie trzeba było pamiętać, że coś z czymś jest sklejone)?

Wskazówka: Wskazówki do tego zadania znajdziecie na końcu skryptu.

6 Proponowane zadania domowe

Zadanie 19 (za 2 punkty)

Korzystając z Małego Twierdzenia Fermata udowodnij, że:

a) $9^{32} - 2 \cdot 9^{16} \equiv 16 \pmod{17}$

b) $8^{24} \equiv 1 \pmod{35}$

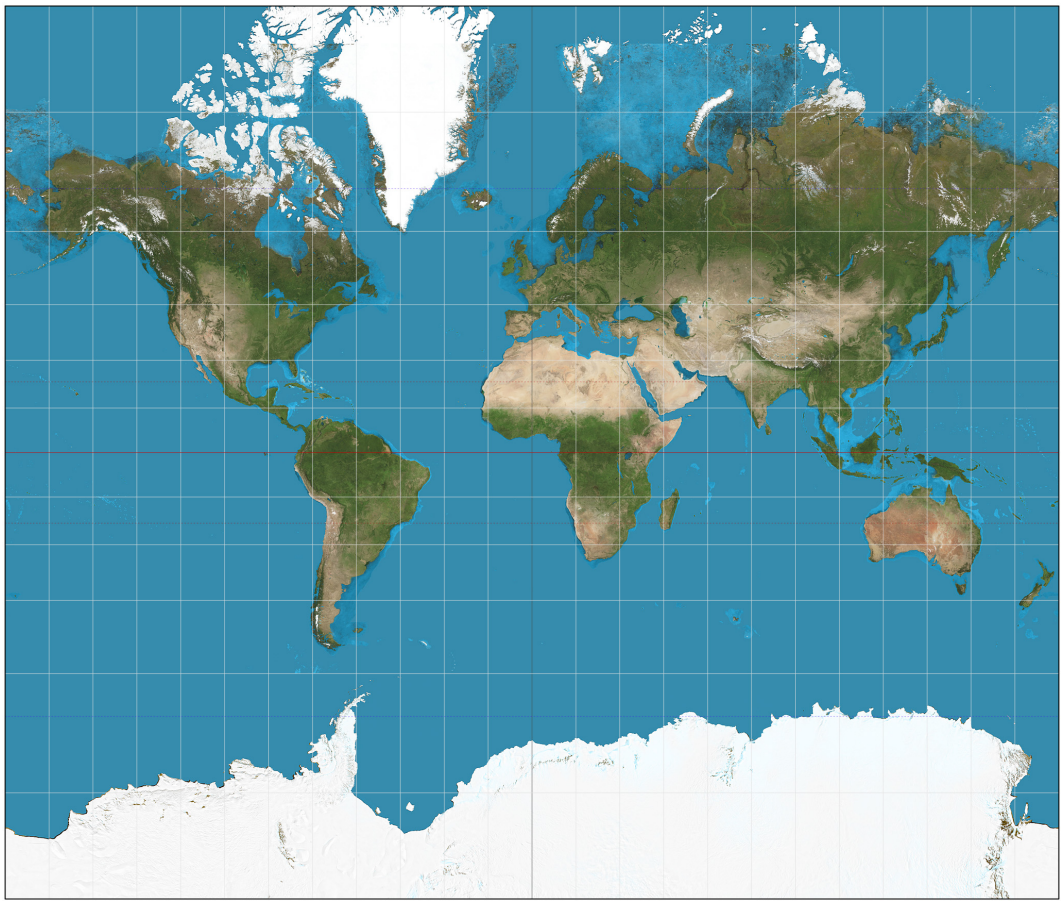
Wskazówka: Wskazówki do tego zadania znajdziecie na końcu skryptu.

Zadanie 20 (za 3 punkty)

Niech p będzie liczbą pierwszą i nie dzieli a. Udowodnij, że najmniejsza liczba $k > 0$, dla której $a^k \equiv 1 \pmod{p}$ jest dzielnikiem liczby $p - 1$.

Zadanie 21 (za 1 punkt)

Na poniższej mapie (odwzorowanie Merkatora) zaznacz najkrótszą trasę pomiędzy Warszawą i Tokio oraz pomiędzy Warszawą a Buenos Aires. Do jej znalezienia możesz użyć globusu i nitki, albo skorzystać z darmowego programu Google Earth (w którym można zobaczyć kulę ziemską oraz wyznaczać proste). Znajdź kąty pomiędzy znalezioną trasą a kierunkiem północnym wyznaczanym przez kolejne zaznaczone na mapie południki. Co zaobserwowałaś/eś?



7 Wskazówki do niektórych zadań

Zadanie 3

Wskazówka: Trzeba zastosować fakt, że dla dowolnego nieparzystego n, $a^n + b^n$ jest podzielne przez $a+b$. Ponadto $3^3 + 4^3 = 7 \cdot 13, 3^5 + 4^5 = 7 \cdot 181, 3^7 + 4^7 = 49 \cdot 379$.

Zadanie 4

Wskazówka: W geometrii euklidesowej suma kątów w trójkącie to $180°$.

Zadanie 5

Wskazówka: Użyjcie trójkątów

Zadanie 13

Wskazówka: Rozłóż wykładniki na czynniki.

Zadanie 15

Wskazówka: $221 = 10 \cdot 22 + 1$

Zadanie 18

Wskazówka: Ustaw tak to koło, które wycinamy, aby przechodziło przez brzeg półsfery.

Zadanie 19

Wskazówka: $35 = 5 \cdot 7$

Zadanie 20

Wskazówka: Niech $p - 1 = nk + r$*. Zauważ, że z Małego Twierdzenia Fermata mamy* $a^k \equiv a^{nk+r} \equiv 1 \pmod{p}$*. Z tego wywnioskuj, że* $r = 0$*.*