Rozgrzewka (Ci, którzy znają pojęcie kongruencji niech przejdą do zadania 3 bc i 4, jeśli i te zadania są za proste to proponuje zadanie 5):

Zad.1

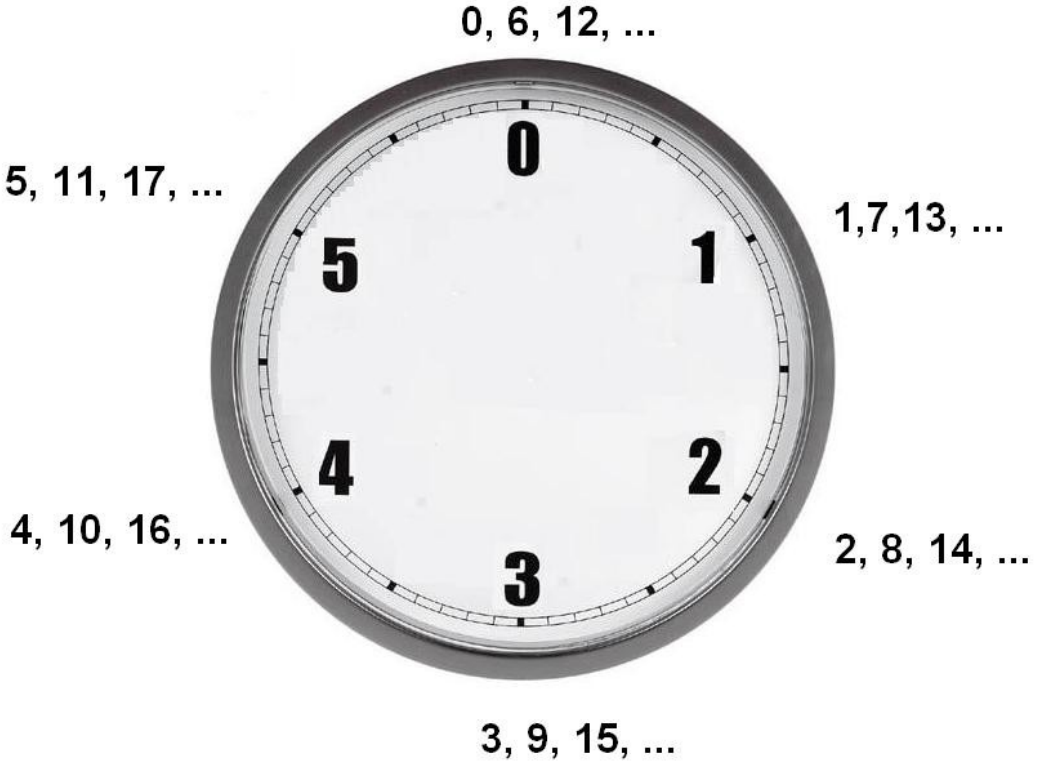
a) Marek wyjechał pociągiem do Warszawy o godzinie 21 i jechał 8 godzin, o której godzinie dojechał na miejsce?

b) Jest godzina 16, którą godzinę po południu mamy?

c) 12 mod 10, 14 mod 7, 25 mod 8

Zad. 2

Na zegarze jest godzina 10.45 lekcja trwa 45, gdzie znajdować się będzie wskazówka minutowa?



Zegar ten przedstawia reszty z dzielenia przez 6. Obrazuje on jak kolejne liczby można przyporządkować do odpowiednich pokazanych na zegarze grup.

Przypomnienie teorii z wykładu :

Systemy liczbowe

Zapis w systemie dziesiątkowym: $16 = 1 \cdot 10^1 + 6 \cdot 10^0$

a w systemie dwójkowym $16 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$ czyli w zapisie binarnym 10000

Co to są kongruencje?

Kongruencja to sposób zapisu tego, że pewne dwie liczby całkowite a i b dają tę samą resztę przy dzieleniu przez liczbę naturalną m. W postaci kongruencji zapisuje się to tak: $a \equiv b \pmod m$.
Bardziej ścisła definicja kongruencji: $a \equiv b \pmod m$ (*a przystaje do b modulo m*), jeśli liczba a − b dzieli się przez m. (a i b są tu liczbami całkowitymi, natomiast m – liczbą naturalną)
Kongruencje pozwalają krótko i elegancko zapisywać rozwiązania zadań o podzielności liczb.

Własności kongruencji:

Notacja $a \equiv b$ ma część własności analogicznych do własności zwykłej równości.
a) jest to **relacja równoważności,** zatem spełnia warunki:
-1- $a \equiv a \pmod m$. **(zwrotność)**
-2- Jeśli $a \equiv b \pmod m$, to $b \equiv a \pmod m$. **(symetria)**
-3- Jeśli $a \equiv b \pmod m$ i $b \equiv c \pmod m$, to $a \equiv c \pmod m$. **(przechodniość)**
b) działania na kongruencjach:
Jeśli $a \equiv b \pmod m$ oraz c jest dowolną liczbą calkowitą, to:
$a + c \equiv b + c \pmod m$, $a - c \equiv b - c \pmod m$, $a * c \equiv b * c \pmod m$.
Ogólniej: Kongruencje o tym samym module można dodawać, odejmować i mnożyć stronami, tzn.:
Jeśli $a \equiv b \pmod m$ i $c \equiv d \pmod m$, to:
$a + c \equiv b + d \pmod m$, $a - c \equiv b - d \pmod m$, $a * c \equiv b * d \pmod m$, $a^n \equiv b^n \pmod m$

Zad. 3 (własności kongruencji)

Dla następujących kongruencji :
[I] $8 \equiv 1 \pmod 7$,
[II] $12 \equiv 5 \pmod 7$,
[III] $10 \equiv 3 \pmod 7$,
przeprowadź dodawanie, odejmowanie, mnożenie jednej kongruencji przez drugą i potęgowanie stopnia drugiego.

a) Oblicz

8+12 (mod 7)	$12^2 \pmod 7$	10 – 12 (mod 7)	10*3 (mod 7)
1+ 5 (mod 7)	$5^2 \pmod 7$	3 – 5 (mod 7)	3*3 (mod 7)

b) Podaj przykład na to, że dzielenie prowadzi do błędnego wyniku.

c) Udowodnij korzystając z definicji własność mnożenia: $a * c \equiv b * d \pmod m$,

Zad. 4

a) Jak obliczyć ostatnią cyfrę liczby 3^{100}.

b) Obliczyć $40^7 \ mod \ 143$

Zad. 5 *

Udowodnij, że $10 \mid 53^{53} - 33^{33}$.

RSA
1) losujemy dwie duże liczby pierwsze p i q
2) losujemy e względnie pierwszą z (p-1)(q-1)
3) obliczamy d = e^{-1} mod (p-1)(q-1) [np. za pomocą rozszerzonego algorytmu Euklidesa]
4) klucz publiczny to para (e, n) gdzie n = pq
5) klucz prywatny to para (d, n)
6) szyfrowanie to c = m^e (mod n)
7) deszyfrowanie $c^d = m^{ed}$ = m (mod n)

Rozszerzony algorytm Euklidesa NWD a i b
wlasnosc p*a0 + q*b0 = a r*a0 + s*b0 = b

```
a0 := a; b0:=b;
p :=1; q:=0; r:=0; s:=1;
while (b != 0) {
    c := a mod b
    quot := a div b
   a:= b;  b:= c;
   new_r := p – quot*r;
   new_s := q – quot*s;
   p:=r; q:=s;
   r:= new_r; s:= new_s
}
```

Zad 6 RSA*
Udowodnij, że $c^d = m^{ed}$ = m (mod n)

Korzystając z podpowiedzi:

Tw. Fermata (małe)
p – pierwsza; a – dowolna calkowita : $a^p - a \equiv 0 (mod\ p)$ czyli $a^{p-1} \equiv 1 (mod\ p)$

Tw. (chinskie o resztach)
Uklad:
x = y1 (mod n1)
x = y2 (mod n2)
...
x = yk (mod nk)
gdzie y1, ..., yk dowolne całkowite n1,n2, ..., nk parami względnie pierwsze
spełnia dokładnie jedna liczba x w przedziale <1, n1*n2*...*nk>

(zob. przykładowa tabelka – *obrazuje ona, że rzeczywiście liczbę znając odpowiednie reszty można wyznaczyć jednoznacznie*)

Tabela 1.

Liczba n	*n modulo 5*	*n modulo 7*
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	0	5
6	1	6
7	2	0
8	3	1
9	4	2
10	0	3
11	1	4
12	2	5
13	3	6
14	4	0
15	0	1
16	1	2
17	2	3
18	3	4
19	4	5
20	0	6
21	1	0
22	2	1
23	3	2
24	4	3
25	0	4
26	1	5
27	2	6
28	3	0
29	4	1
30	0	2
31	1	3
32	2	4
33	3	5
34	4	6

Reszty z dzielenia liczb *0,1 2 ,...,34* przez *5 i 7*

Zad 7 RSA (rachunkowe)
p = 11, q =13, e =7

a) oblicz d (patrzac na alg Euklidesa)

Rozwiązania / szkice rozwiązań / wskazówki :

ad 1.
a) (działanie modulo 24) $21 + 8 \equiv 5 \pmod{24}$, b) 16 (mod 12)

ad 2.
10.45 + 45 = 11.30 45 + 45 (mod 60) = 30

ad 3.
a) patrząc na kolejne pary widzimy, że własności są prawdziwe
przykładowo $10-12 \equiv -2 \equiv 5 (mod\ 7)$ podobnie dla $3-5 \equiv 5 (mod\ 7)$ pokazują nam odejmowanie kongruencji [III] - [II].
Ujemne wartości możemy wyobrazić sobie cofając się na zegarze.

b) $4 \equiv 12 (mod\ 8)$ jest prawdziwe; $2 \equiv 6 (mod\ 8)$ **FAŁSZ !**
Zauważmy, że $2*2 \equiv 6*2 (mod\ 4*2)$ oraz $2 \equiv 6 (mod\ 4)$
Tw. Jeśli d jest dowolną liczbą naturalną, to $ad \equiv bd (mod\ md)$, wtedy i tylko wtedy, gdy $a \equiv b (mod\ m)$
Bo: m|a − b wtedy i tylko wtedy gdy md|(a − b)d.
c) Skoro m|a − b oraz m|c − d, więc też m|ac − bd = (a − b)c + (c − d)b.

ad 4.
zauważmy, że reszty występują cyklicznie
a) mamy 3, 9, 27, 81, 243, … czyli (mod 10) kolejno 3, 9, 7, 1, 3, 9, …..
b) 105

ad 5.
Należy udowodnić, że $53^{53} - 33^{33} \pmod{10}$.
Wpierw sprawdźmy, do ilu przystaje $53^{53} \pmod{10}$:
$53 \equiv 3 \pmod{10}$, więc $53^{53} \equiv 3^{53} \pmod{10}$.
Zobaczmy więc, do ilu przystaje $3^{53} \pmod{10}$.
$3^1 \equiv 3 \pmod{10}$
$3^2 \equiv 9 \pmod{10}$
$3^3 \equiv 27$ czyli 7 (mod 10)
$3^4 \equiv 1 \pmod{10}$
Zatem $3^{53} \equiv (3^4)^{14} * 3 \equiv 1^{14} * 3 \equiv 3 \pmod{10}$
Więc również $53^{53} \equiv 3 \pmod{10}$.
Podobnie sprawdzamy, do ilu przystaje $33^{33} \equiv 3$

ad 6
ponieważ e jest odwrotnością d mod (p-1)(q-1) to istnieje takie k, że : ed = 1 + k (p-1)(q-1)
jeśli $m \equiv 0 (mod\ p)$ to $m^{ed} \equiv 0 (mod\ p)$ czyli $m^{ed} \equiv m (mod\ p)$
jeśli $m \equiv jakasliczba (mod\ p)$ i $jakasliczba \neq 0$, to korzystając z Małego Tw. Fermata mamy:
$m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m(m^{p-1})^{k(q-1)} \equiv m(1)^{k(q-1)} \equiv m (mod\ p)$
Podobnie pokazujemy dla q. I z chinskiego tw. o resztach mamy $m^{ed} \equiv m \pmod{n}$.
[bo n=pq, założenia tw. są spełnione - sprawdź]

ad 7.
120 mod 7 = 1 ; quot = 17 ; a=7 b=1 r =1-17*0 s=-17 p=0 q=1
7 mod 1 = 0 ; quot = 7 ; a =1 b =0 r = -7 s=1+17*7 p=1 q=-17
NWD (7, 120) = 1 * 120 + (-17)*7 i mamy -17=103 (mod 120) = d