Модулярная арифметика

Алфавит

$A \leftrightarrow 0$	$B \leftrightarrow 1$	$C \leftrightarrow 2$	$D \leftrightarrow 3$	$E \leftrightarrow 4$	$F \leftrightarrow 5$	$G \leftrightarrow 6$
$H \leftrightarrow 7$	$I \leftrightarrow 8$	$J \leftrightarrow 9$	$K \leftrightarrow 10$	$L \leftrightarrow 11$	$M \leftrightarrow 12$	$N \leftrightarrow 13$
$O \leftrightarrow 14$	$P \leftrightarrow 15$	$Q \leftrightarrow 16$	$R \leftrightarrow 17$	$S \leftrightarrow 18$	$T \leftrightarrow 19$	$U \leftrightarrow 20$
	$V \leftrightarrow 21$	$W \leftrightarrow 22$	$X \leftrightarrow 23$	$Y \leftrightarrow 24$	$Z \leftrightarrow 25$	

1. *Шифр Цезаря.* Используя шифр Цезаря, т.е. сдвиг на 3 позиции, и приведенный выше алфавит, зашифруйте сообщение

   `DURA LEX SED LEX.`

   А что получится, если использовать сдвиг на 26 позиций? 29 позиций?

2. Говорят, что целые числа a и b сравнимы по модулю натурального числа n, если $a - b$ делится на n. Обозначается $a \equiv b \pmod{n}$.

   (a) Покажите, что a и b сравнимы по модулю натурального числа n тогда и только тогда, когда a и b дают одинаковые остатки при делении на n.

   (b) Покажите, что если $a_1 \equiv b_1 \pmod{n}$, $a_2 \equiv b_2 \pmod{n}$, то $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ и $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

3. *Аддитивный шифр.* Сообщение

   `HPWWOZYPLWPI`

   зашифровано при помощи аддитивного шифра $X \mapsto X + 11 \pmod{26}$. Известно, что последние четыре буквы — это подпись ALEX. Расшифруйте сообщение.

4. *Мультиплкативный шифр.* Для мультипликативного шифра $X \mapsto kX \pmod{26}$ заполните следующую таблицу:

Открытый текст	A	B	C	D	E	F	G	H	I	J	K	L	M
Позиция k	0	1	2	3	4	5	6	7	8	9	10	11	12
2k (mod **26**)	0	2	4	6	8	10	12	14	16	18	20	22	24
Шифртекст	A	C	E	G	I	K	M	O	Q	S	U	W	Y
3k (mod **26**)	0	3	6	9	12	15	18	21	24	1	4	7	10
Шифртекст	A	D	G	J	M	P	S	V	24	B	E	H	K

Открытый текст	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Позиция k	13	14	15	16	17	18	19	20	21	22	23	24	25
2k (mod **26**)													
Шифртекст													
3k (mod **26**)													
Шифртекст													

   Расшифруйте сообщение a) `NQFDAJ` для $k = 3$; b) `CAG` для $k = 2$.

5. Целые числа a и b называются взаимно обратными по модулю числа $n \in \mathbb{N}$, если

$$ab \equiv 1 \pmod{n}.$$

В этом случае число a называется обратным к числу b по модулю $n \in \mathbb{N}$, а число b называется обратным к числу a по модулю $n \in \mathbb{N}$. Число, обратное к числу a по модулю $n \in \mathbb{N}$, обозначают $a^{-1} \pmod{n}$.

Найдите (если существуют) обратные к числам $2, 3, 5, 7$ по модулю a) $n = 6$; b) $n = 7$; c) $n = 26$.

6. Покажите, что обратное к числу $a \in \mathbb{N}$ по модулю n число существует тогда и только тогда, когда a и n взаимно просты.

7. *Аффинный шифр.* Известно, что сообщение

RGREB QETVR TLJKK SNJTL PGREB JKKQE TVR

зашифровано при помощи аффинного щифра $X \mapsto aX+b \pmod{26}$. Зная, что в открытом тексте дважды встречается слово PRIME (простое число), найдите a и b. Найдите преобразования расшифрования. Расшифруйте сообщение.

Домой

В этом задании все тексты на русском языке, поэтому все вычисления по модулю 32.

1. Сообщение

ТЪЮЯМ ФПСЗС ХРСЧП ЦЩХКЧ ЗЫППЮ МУЦТХ ЬЗЖ

зашифровано при помощи аддитивного шифра. Расшифруйте его.

2. Известно, что сообщение

ВТЭДГ ЗИФЗЩ ЬЗЪЬН ЫЗСИЗ ГИДСЕ ГЕЩНС ЕУНРЬ ЗТЕИЕ ЕИНСВ ГЖВЧИ
БНГУЗ ЭЗСЬН ЮКЬЗО ЗУЭЮЩ НГЫЗУ ЗЭЗСТ ЭЗНЬН ЖЕЪЕЭ ЗГНЬЗ ИУЗХД
ИУБЩД ИВУЭН ЪЖЕКЬ ЦФХЕЙ ЭЗГЗЩ ЬНЫЗВ ГЦЬЮП ЩДЬТЭ ЕЪЬНУ БИВКУ
ЗМУЗУ ХЕЙЭЩ ЖВСДЬ ВИЗГД ЭХДЬЬ НВЬЗГ ЗИУБЯ ДЖБЕЪ ЗШЭДУ НУДЖВ
МУЗРИ ЕИУДС ЦЪНЫЖ ЧКНЖН ИБЗКД ГЕЩЬЗ ГУЗСК УЗШЦИ ЫЭЦУБ КУЗМУ
ЕЪЬНК ЫЕВГЖ ВЧУИВ ТЕИБС ДЬНСЕ ЕГЦЩН УБЕФЪ НЩДУИ ЫЕДЭЕ ИЮЬЫЕ
ЬЗГИВ ЫЕРЫУ ЗЩЗОН ЩНДУИ ВКУЗЪ ЬНКЫЕ МУЕЛИ ЗЗУГД УИУГЮ ЧУШЮЫ
ГНСШД ЪЗИЗШ ЗОЗУЭ ЮЩНЭН ЪОНЩН ДУЕФД ИЖЕГЗ ИТЗЖБ ЪЮДУИ ВЗШЦК
ЬЦСЕТ ЭНГЕЖ НСЕЭН ЪОНЩЦ ГНЬЕВ ХЕЙЭЗГ

зашифровано при помощи аффинного шифра $X \mapsto aX+b \pmod{32}$. Используя частотную таблицу, расшифруйте сообщение.

Алфавит

А ↔ 0	Б ↔ 1	В ↔ 2	Г ↔ 3	Д ↔ 4	Е ↔ 5	Ж ↔ 6	З ↔ 7
И ↔ 8	Й ↔ 9	К ↔ 10	Л ↔ 11	М ↔ 12	Н ↔ 13	О ↔ 14	П ↔ 15
Р ↔ 16	С ↔ 17	Т ↔ 18	У ↔ 19	Ф ↔ 20	Х ↔ 21	Ц ↔ 22	Ч ↔ 23
Ш ↔ 24	Щ ↔ 25	Ъ ↔ 26	Ы ↔ 27	Ь ↔ 28	Э ↔ 29	Ю ↔ 30	Я ↔ 31

Буквы русского языка, упорядоченные по частотности в порядке убывания:

О Е А И Н Т С Р В Л К М Д П У Я Ы Ь Г З Б Ч Й Х Ж Ш Ю Ц Щ Э Ф Ъ Ё