Глава 1

Задачи

1. На первой лекции рассматривался вопрос о том, как Алиса может переслать секретное сообщение Бобу. При этом Алиса использовала ключи 7 и 43, а у Боба были свои ключи 3 и 67.

1.1. Определите все числа a из промежутка $2 \leqslant a < 1000$, которые Алиса может секретно переслать Бобу при использовании тех же четырёх ключей.

1.2. Может ли Боб отправлять секретные сообщения Алисе, если они будут пользоваться теми же своими четырьмя ключами?

1.3. Какие ключи может выбирать Боб так, чтобы он смог прочитать любое сообщение Алисы, использующей те же ключи 7 и 43.

1.4. Какие рекомендации по выбору ключей Вы могли бы дать Алисе и Бобу с тем, чтобы они могли обмениваться секретной информацией указанным способом.

1.5. Как следует выбирать ключи, если модуль, по которому выполняются все вычисления, равен 10^4.

2. Пусть a, n - целые числа, $n \geqslant 4$, $a \geqslant 1$.

2.1. Докажите, что при любом a, не делящемся на 5 выполняется сравнение

$$a^{4 \cdot 5^{n-1}} \equiv 1 \pmod{5^n}.$$

2.4. Как нужно выбирать ключи, если Алисе и Бобу захочется обмениваться секретной информацией при каком-либо модуле вида $5^n, n \geqslant 4$.

2.5. В дальнейшем для всех a, не делящихся на 5 будет использоваться функция

$$Q(a) \equiv \frac{a^{100} - 1}{125} \pmod{125}, \qquad 0 \leqslant Q(a) < 125.$$

См. задачу 2.1. Докажите, что если целые числа a, b не делятся на 5, то

$$Q(ab) \equiv Q(a)Q(b) \cdot \pmod{5^n}.$$

2.6. Докажите, что значение $Q(3)$ не делится на 5.

2.7. Докажите, что при любых a, b, не делящихся на 5, и с условием $5 \nmid Q(b)$, системе сравнений

$$\begin{cases} Q(b)x \equiv Q(a) \pmod{125}; \\ x \equiv x_0 \pmod{4}; \end{cases} \tag{1.1}$$

где x_0 есть единственное целое число, удовлетворяющее условиям

$$a \equiv b^{x_0} \pmod{5}, \qquad 0 \leqslant x_0 < 4,$$

удовлетворяет единственное целое число, принадлежащее промежутку $0 \leqslant x < 500$. Оно удовлетворяет также сравнению

$$b^x \equiv a \pmod{625}. \tag{1.2}$$

Заметим, что система сравнений (1.1) легко может быть решенаю И это даёт возможность быстрого решения сравнения. Подобная конструкция может быть использована и для модулей вида p^n при сравнительно небольших p и сколь угодно больших n.

2.8. Придумать способ быстрого решения показательных сравнений по модулю 10^n.

2.9. Алиса и Боб установили секретную переписку, пользуясь сравнениями по модулю $5^4 = 625$ и действуя так же, как в задаче 1. Злонамеренная Ева решила узнать секреты Алисы и Боба. С этой целью она перехватила 3 засекреченных варианта одного и того же письма, пересылаемых сначала от Алисы к Бобу, затем от Боба к Алисе и ещё раз от Алисы к Бобу:

$$A \xrightarrow{347} \text{Б} \xrightarrow{602} A \xrightarrow{153} \text{Б}. \tag{1.3}$$

Пользуясь этой информацией Ева смогла определить ключи, использованные Алисой и Бобом, а также прочитать зашифрованное сообщение. Вы также можете сделать это, воспользовавшись конструкцией из задачи 2.7.

Подсказка. Попробуем определить один из ключей Боба. Обозначим его $x_\text{Б}$. Из картинки (1.3) следует, что $347^{x_\text{Б}} \equiv 602 \pmod{625}$. Это сравнение совпадает со сравнением (1.2) при $a = 602$ и $b = 347$. Эти числа не делятся на 5, а кроме того, $Q(b) \equiv \frac{347^{100}-1}{125} \pmod{125} \equiv 41 \pmod{125}$ также не делится на 5. Справедливы сравнения $602 \equiv 2 \pmod 5$ и $347 \equiv 2 \pmod 5$, из них следует, что $2^{x_0} \equiv 2 \pmod 5$ и $x_0 = 1$. Согласно утверждению задачи 2.7 для нахождения ключа $x_\text{Б}$ достаточно решить систему сравнений

$$\begin{cases} 41x & \equiv 8 \pmod{125}; \\ x & \equiv 1 \pmod 4. \end{cases}$$

Здесь используется равенство $Q(602) = 8 \pmod{125}$. Первое сравнение имеет решение $x \equiv 113 \pmod{125}$. Так как $113 \equiv 1 \pmod 4$, заключаем, что полученная система имеет единственное решение $x \equiv 1 \pmod{500}$ на промежутке $0 \leqslant x < 500$, а именно $x = 113$. Но тогда $x_{\text{Б}} = 113$, ключ Боба для шифрования равен 113. Далее можно действовать примерно так же.