Занятия 24, 25 и 26 (10/12/2007, 15/12/2007 и 17/12/2007)
Приведенная система вычетов. Теорема Эйлера.

***Определение* 1.** Пусть m — некоторое натуральное число. Рассмотрим $r_1, r_2, \ldots, r_n$ — все вычеты, взаимно простые с m. Набор таких вычетов называется приведённой системой вычетов.

Заметим, что с приведённой системой вычетов можно совершать операции умножения и деления. Действительно, если a и b — два вычета из приведённой системы, то $(a \cdot b, m) = 1$ и сравнение $ax \equiv b \pmod m$ разрешимо, причём результат будет взаимно прост с m (проверьте). Операции сложения и вычитания совершать нельзя, так как результат может не принадлежать приведённой системе вычетов (приведите пример).

***Определение* 2.** Количество вычетов по модулю m, взаимно простых с m, будем обозначать $\varphi(m)$. Функция $\varphi(m)$ называется функцией Эйлера.

4.60. Постройте приведённую систему вычетов по модулю а) 12; б) 9; в) 7.

4.61. Вычислите а) $\varphi(5)$; б) $\varphi(p)$; в) $\varphi(p^2)$; г) $\varphi(pq)$, где p и q — простые числа.

4.62. Пусть $a \cdot r \equiv b \cdot r \pmod m$ и $(r, m) = 1$. Докажите, что $a \equiv b \pmod m$.

4.63. Пусть $r_1, r_2, \ldots, r_n$ — приведённая система вычетов по модулю m, a — некоторое число, взаимно простое с m. Докажите, что набор $a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_n$ — тоже приведённая система вычетов.

4.64. Обозначим $r = r_1 \cdot r_2 \cdot \ldots \cdot r_n$. Набор $ar_1, ar_2, \ldots, ar_n$ — приведённая система вычетов, то есть это те же самые вычеты, просто как-то переставленные. Поэтому

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_n \equiv r \pmod m.$$

Докажите, что $a^n r \equiv r \pmod m$.

4.65. Пользуясь предыдущей задачей, докажите, что $a^n \equiv 1 \pmod m$.

***Теорема* 1.** *Теорема Эйлера*

$\Diamond$ *Пусть* $(a, m) = 1$, *тогда*

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

$\blacklozenge$

4.66. Найдите остаток от деления 128^{2007} на 125

4.67. Докажите, что для любого нечётного числа m существует натуральное n такое, что $(2^n - 1) \vdots m$.

4.68. Докажите, что при любом нечётном n $\left(2^{n!} - 1\right) \vdots n$.

4.69. Для взаимно простых m и n рассмотрим таблицу:

1	2	3	$\ldots$	n
$n+1$	$n+2$	$n+3$	$\ldots$	$2n$
$2n+1$	$2n+2$	$2n+3$	$\ldots$	$3n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$(m-1)n+1$	$(m-1)n+2$	$(m-1)n+3$	$\ldots$	mn

а) Докажите, что если в столбце верхнее число взаимно просто с n, то и все числа столбца взаимно просты. И наоборот, если верхнее число не взаимно просто с n, то и все числа столбца с n не взаимно просты.
б) Докажите, что любые два числа, стоящие в одном столбце, дают разные остатки при делении на m.
в) Сколько в каждом столбце чисел, взаимно простых с m?
г) Свойство мультипликативности Докажите, что если m и n взаимно просты,то $\varphi(mn) = \varphi(m)\varphi(n)$.