1. Сравнения.

m— натуральное число, x, y— целые. Сравнение $x \equiv y(\mathrm{mod} m)$ означает, что $x - y$ делится на m. Свойства: эквивалентность; цепочки сравнений. $x \equiv y(\mathrm{mod} m)$ равносильно тому, что x и y имеют одинаковый остаток при делении на m. Почленное сложение, вычитание, умножение, возведение в степень, деление на число, взаимно простое с модулем. Пример:

$$3^{16} = (3^2)^8 = 9^8 = (9^2)^4 = 81^4 \equiv 12^4 = (12^2)^2 = 144^2 \equiv 6^2 = 36 \equiv 13(\bmod 23).$$

2. Малая теорема Ферма.

Пусть p— простое, a не делится на p. Тогда $a^{p-1} \equiv 1(\mathrm{mod} p)$.

Доказательство. Пусть r_k— остаток при делении ka на p. Имеем

$$1 \times a \equiv r_1(\mathrm{mod} p),$$

$$2a \equiv r_2(\mathrm{mod} p),$$

$$\ldots,$$

$$((p-1)a \equiv r_{p-1}(\mathrm{mod} p).$$

Если $r_k = r_l$, то $ka \equiv la(\mathrm{mod} p)$, $k \equiv l(\mathrm{mod} p)$, $k = l$. Значит, $r_1, r_2, \ldots, r_{p-1}$ различны и пробегают все числа $1, 2, \ldots, p-1$. Следовательно,

$$(p-1)!a^{p-1} \equiv (p-1)!(\mathrm{mod} p),$$

$$a^{p-1} \equiv 1(\mathrm{mod} p).$$

3. Частный случай теоремы Эйлера.

p, q— различные простые числа, $(a, pq) = 1$. Тогда $a^{(p-1)(q-1)} \equiv 1(\mathrm{mod}\ pq)$. Действительно,

$$a^{(p-1)(q-1)} = (a^{p-1})^{q-1} \equiv 1^{q-1} = 1(\mathrm{mod} p)$$

,

$$a^{(p-1)(q-1)} = (a^{q-1})^{p-1} \equiv 1^{p-1} = 1(\mathrm{mod} q)$$

, откуда $a^{(p-1)(q-1)}$ делится на pq.

4. Приложение к криптографии.

5. Малая теорема Ферма— не достаточное условие простоты.

Если p— простое число, $p \geq 5$, то число $n = (2^{2p} - 1)/3$ составное, но $2^{n-1} \equiv 1(\mathrm{mod} n)$. Действительно,

$$2^p = 2 \times (2^2)^{(p-1)/2} \equiv 2 \times 1^{(p-1)/2} = 2(\mathrm{mod} 3),$$

$$n = (2^p - 1)((2^p + 1)/3).$$

Значит, n— составное. Далее,

$$2^{2p} = 2^2 \times (2^{p-1})^2 \equiv 4 \times 1^2 = 4(\mathrm{mod} p).$$

Значит, $2^{2p}-4$ делится на $2p$. Так как $p>3$, то $n-1=(2^{2p}-4)/3$ также делится на $2p$. Следовательно,

$$2^{n-1}=(2^{2p})^{(n-1)/(2p)}\equiv 1^{(n-1)/(2p)}=1(\mathrm{mod}(2^{2p}-1)).$$

Итак, $2^{n-1}-1$ делится на $2^{2p}-1=3n$.

6. Вариант необходимого условия: возведение в степень $(n-1)/2$.

Если $n>2$— простое число, a не делится на n, то $a^{(n-1)/2}\equiv\pm 1(\mathrm{mod} n)$. Действительно,

$$a^{n-1}-1=(a^{(n-1)/2})^2-1=(a^{(n-1)/2}-1)(a^{(n-1)/2}+1),$$

и по малой теореме Ферма одно из чисел $a^{(n-1)/2}-1$, $a^{(n-1)/2}+1$ делится на n.

7. Формулировка достаточного условия простоты.

Теорема. Если $n=2^sk+1$, $k\le 2^s$, $a^{(n-1)/2}\equiv -1(\mathrm{mod} n)$, то n— простое. Для простого n найти подходящее a довольно просто. Например, если k не делится на 3, то сравнению удовлетворяет $a=3$, и мы получаем критерий простоты чисел вида $n=2^sk+1$, $k\le 2^s$, k не делится на 3.

8. Порядок элемента по модулю p.

Лемма 1. Пусть p— простое, a не делится на p, $M=\{m>0 : a^m\equiv 1(\mathrm{mod} p)\}$, m_0— наименьший элемент M. Тогда M состоит из натуральных чисел, кратных m_0.

Доказательство. Если m делится на m_0, то

$$a^m=(a^{m_0})^{m/m_0}\equiv 1^{m/m_0}=1(\mathrm{mod} p),$$

т.е. $m\in M$. Обратно, пусть $m\in M$, r— остаток при делении m на m_0. Тогда $m=lm_0+r$ и

$$1\equiv a^m=(a^{m_0})^l a^r\equiv a^r(\mathrm{mod} p),$$

и по выборы m_0 случай $1\le r<m_0$ невозможен, т.е. $r=0$ и m делится на m_0.

9. Лемма о простых делителях.

Лемма 2. Если $n=2^sk+1$, $a^{(n-1)/2}\equiv -1(\mathrm{mod} n)$,то любой простой делитель p числа n удовлетворяет сравнению $p\equiv 1(\mathrm{mod} 2^s)$.

Доказательство. Пусть $M=\{m>0 : a^m\equiv 1(\bmod p)\}$, m_0— наименьший элемент M. Пусть 2^t— наибольшая степень двойки, делящая m_0; тогда $m_0=2^tl$, где l— нечетное число. Так как $n-1\in M$, то по лемме 1 m_0 делит $n-1$; значит, l делит k. Допустим, что $t<s$. Тогда $(n-1)/2=2^{s-1}k$ делится на $m_0=2^tl$. По лемме 1 $(n-1)/2\in M$, но это не так. Значит, $t\ge s$. По малой теореме Ферма $p-1\in M$, и по лемме 1 $p-1$ делится на m_0, а значит, и на 2^s.

10. Доказательство теоремы.

Допустим, что число n не простое, тогда у него имеется простой делитель $p\le\sqrt{n}$. По лемме 2 $p\ge 2^s+1$, откуда $n\ge(2^s+1)^2$. С другой стороны, $n=2^sk+1\le(2^s)^2+1$— противоречие.