
N0C7FN0LIF3
клуб по информационной безопасности*

Простое число

Это Натуральное число, имеющее ровно два различных натуральных делителя - единицу и самого себя.

Таблица простых чисел

2	79	191	311	439	577	709	857
3	83	193	313	443	587	719	859
5	89	197	317	449	593	727	863
7	97	199	331	457	599	733	877
11	101	211	337	461	601	739	881
13	103	223	347	463	607	743	883
17	107	227	349	467	613	751	887
19	109	229	353	479	617	757	907
23	113	233	359	487	619	761	911
29	127	239	367	491	631	769	919
31	131	241	373	499	641	773	929
37	137	251	379	503	643	787	937
41	139	257	383	509	647	797	941
43	149	263	389	521	653	809	947
47	151	269	397	523	659	811	953
53	157	271	401	541	661	821	967
59	163	277	409	547	673	823	971
61	167	281	419	557	677	827	977
67	173	283	421	563	683	829	983
71	179	293	431	569	691	839	991
73	181	307	433	571	701	853	997

Взаимно-простые числа

Целые числа ***взаимно просты***, если их наибольший общий делитель равен 1. Например, взаимно просты числа 14 и 25, так как у них нет общих делителей; но числа 15 и 25 не взаимно просты, так как у них имеется общий делитель 5.

Сравнение

Целые числа a и b называют сравнимыми по модулю m, если каждое из них при делении на m дает один и тот же остаток r.

$r \equiv a \pmod{m}$.
$r \equiv b \pmod{m}$.

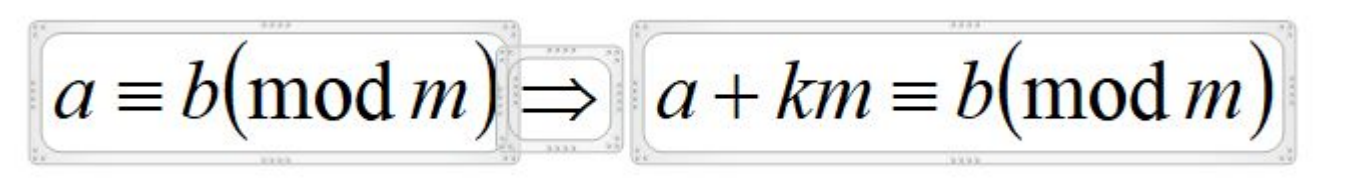
То есть существует такое число t такое , что выполняется равенство
$r \equiv a + m*t$
$r \equiv b + m*t$
Пример:
$125 \equiv 13 \pmod{16}$
Или
125 = 13 + 16*t, где если t=7, выполнено равенство

Если $a \equiv b(mod\ n)$ и $d \equiv c(mod\ n)$, то:

1) $a + d \equiv b + c(mod\ n);$
2) $a \cdot d \equiv b \cdot c(mod\ n);$
3) $a \cdot k \equiv b \cdot k(mod\ n \cdot k);$
4) $a + k \equiv b + k(mod\ n);$
5) $a^m \equiv b^m(mod\ n);$
6) $a + t_1 \equiv b + t_2(mod\ n), t_1 \vdots n, t_2 \vdots n;$
7) $a : k \equiv b : k(mod\ n), \text{НОД}\ (k, n) = 1;$
8) $a : k \equiv b : k(mod\ n : k);$
9) $a \equiv b(mod\ t), n \vdots t.$

Теорема

В любой части сравнения можно отбросить или добавить слагаемое, кратное модулю.



Пример

13 ≡ 125(mod 16)
13 + 16*k ≡ 125(mod 16)
Пусть k = 1
13+ 32 ≡ 125(mod 16)
45 ≡ 125(mod 16)

Доказательство

Представим сравнение в виде уравнения с одной переменной:

$45 = 125 + m*t$

Если взять $t = -5$ получим:

$45 = 125 – 5*16$

Верно

Задачи

1)Найдите остаток от деления 22^9 на 11.

2) Найдите остаток от деления 34^{12} на 11

3)Найдите остаток от деления 2^{29} на 11.

Функция Эйлера

$\varphi(n)$ (функция Эйлера) – это количество чисел из ряда 0,1,2,3,...,n-1, взаимнопростых с числом «**n**»

Любое число можно представить в виде множителей состоящих из простых чисел

$n = p_1^{a1} * p_2^{a2} * \ldots * p_k^{ak}$

$\varphi(n) = n * (1 - 1/p_1) * (1 - 1/p_2) * (1 - 1/p_3) * \ldots * (1 - 1/p_k)$

в

Теорема Эйлера

Пусть m > 1, НОД(a,m) = 1, ϕ(m)-функция Эйлера

Справедливо следующее

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

Теорема Ферма:
Пусть p – простое число и оно не делит «a», то верно следующее:

$$a^{p-1} = 1 \pmod{p}$$

Задачи

1)Девятая степень однозначного числа оканчивается на цифру 7

2) Найти 2 последние цифры числа 243^{402}

3)Доказать что:

$1^{18}+ 2^{18}+ 3^{18}+ 4^{18}+ 5^{18}+ 6^{18} \equiv -1 (\mathrm{mod}\ 7)$

Алгоритм Евклида

Для нахождения наибольшего общего делителя двух чисел a и b (a и b – целые положительные числа, причем a больше или равно b) последовательно выполняется деление с остатком, которое дает ряд равенств вида

Суть алгоритма заключается в том, чтобы последовательно проводить деление с остатком.
Представим a = b*q+r ,
НОД(a,b) = НОД(b,r) и так далее пока вторым число не будет ноль
НОК(a,b)= (a*b)/НОД(a,b)

Алгоритм Евклида

Пример:

Найдите наибольший общий делитель чисел 64 и 48.

Решение

Введем обозначения: a = 64 , b = 48

НОД(64,48)= НОД(48,(64mod48))=НОД(16,(48mod16))=НОД(16,0)

Ответ: Наибольший общий делитель равен 16

Теорема Безу

Если «a» и «b» не равны 0, то существуют такие коэффициенты «x» и «y», такие что:

НОД(a,b)=a*x+b*y

Обратный элемент по модулю

Если число «a» принадлежит Z_m (кольцу целых чисел по модулю m), то мултипликативным обратным по модулю к числу «a» называется число «a^{-1}» принадлежащее Z_m, где выполняется :

$$a*a^{-1} \equiv 1 (\mathrm{mod}\ m)$$

То есть НОД(a,a^{-1})=1

Для элементов кольца $a \in Z_m$ и НОД(a,m)=1 справедливо следующее:

$$a^{-1} \equiv a^{\phi(m)-1} (\mathrm{mod}\ m)$$

Или можно найти обратное через теорему Безу, то есть найти коэффициенты x,y для уравнения, где «x» и есть обратное:
ax+my=d ,но если d>1, то обратного не существует.