основание? Запишем

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k \quad (\text{где } a_i < p)$$

и обозначим

$$\sigma_p(n) = a_0 + a_1 + a_2 + \ldots + a_k,$$

получается красивая

Теорема 1. *$n - \sigma_p(n)$ делится на $(p-1)$.*

Докажем. Это очень просто — рассуждение не меняется: разность

$$n - \sigma_p(n) = (a_0 - a_0) + a_1(p-1) + a_2\left(p^2 - 1\right) + \ldots + a_k\left(p^k - 1\right),$$

разумеется, делится на $(p-1)$.

Например, в восьмеричной системе счисления число, записанное как 124, делится на 7. Проверим?

$$4 + 2 \cdot 8 + 1 \cdot 64 = 84$$

— действительно, на 7 делится. Вот вам и новый признак делимости на 7. Жаль только, что к восьмеричной системе счисления мы не больно-то привычные.

Куда бы дальше пойти? Что бы еще извлечь из делимости? А что если… действительно поделить? В самом деле, вполне достойный вопрос: чему равно частное от деления

$$\delta_p(n) = \frac{n - \sigma_p(n)}{p-1}\ ?$$

Интересно… Начнем хотя бы с $p = 2$, там хоть делить не надо. Составим для начала табличку:

n	n_2	$\sigma_2(n)$	$\delta_2(n) = n - \sigma_2(n)$
0	0	0	0
1	1	1	0
2	10	1	1
3	11	2	1
4	100	1	3
5	101	2	3
6	110	2	4
7	111	3	4
8	1000	1	7
9	1001	2	7
10	1010	2	8
11	1011	3	8
12	1100	2	10

Что мы видим? При переходе от четного n к нечетному число $\delta_2(n)$ не меняется, на четном — меняется. А на сколько? Ага, как раз на столько, сколько нулей в конце двоичной записи числа n. А число это, как известно, есть максимальная степень двойки, на которую делится n. Например, $n = 12$ делится на $4 = 2^2$, и шагнули мы на 2 — от 8 до 10. Значит, мы можем сказать, что $\delta_2(n)$ как бы считает, сколько степеней двойки есть в числах 1, 2,…, n или, лучше сказать, в произведении $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$, которое обозначается обычно $n!$ и называется *факториалом числа n.* Итак, вроде бы верен следующий факт: *$\delta_2(n) = n - \sigma_2(n)$ есть максимальная степень двойки, на которую делится число $n!$.* Докажем?

В бой, ясное дело, просится индукция. Для малых n все видно из таблицы. Давайте осуществим индукционный переход. Допустим, что для $(n-1)$ мы нужный результат уже получили: $(n-1) - \sigma_2(n-1)$ есть максимальная степень двойки, на которую делится число $(n-1)!$. Докажем для n. Число $n!$ отличается от $(n-1)!$ только тем, что оно в n раз больше. Значит, появится ровно столько новых степеней двойки, сколько их есть в числе n, а это как раз число нулей в конце двоичной записи числа n. А как насчет $n - \sigma_2(n)$ по сравнению с $(n-1) - \sigma_2(n-1)$? Само n по сравнению с $n-1$ увеличилось на 1. А как изменится $\sigma_2(n)$ по сравнению с $\sigma_2(n-1)$? Допустим, что в конце двоичной записи числа n стоит k нулей: …1000…0. Тогда $n-1$ имеет вид …0111…1 с k единицами на конце (разве что ноль может и отсутствовать). Значит, единиц стало на $k-1$ меньше, а общее изменение равно $1-(-(k-1))$, что как раз равняется k, и тем самым индукционный переход оказывается верным.

Куда дальше? Ну, конечно, интересно, верно ли это в общем случае, т.е. правда ли, что

$$\delta_p(n) = \frac{n - \sigma_p(n)}{p-1}$$

есть максимальная степень p, делящая $n!$.

Упражнение 1. Докажите это для $p = 3$.

Увы, при $p = 4$ нас ждет разочарование. Число 6! делится на 4^2, но $\delta_4(6) = (6-3)/3 = 1 \neq 2$. Причину мы откроем очень быстро — необходимо, чтобы p было простым.

Упражнение 2. Докажите справедливость утверждения для любого простого p.

К счастью, для решения вопросов о делимости кроме простых чисел нам больше ничего и не нужно. Но что нам делать с факториалами, куда приспособить только что полученные знания? Конечно же, в первую очередь, для биномиальных коэффициентов $C_n^i = \dfrac{n!}{i!(n-i)!}$. Главная формула, с которой они связаны, — это бином Ньютона:

$$(x+y)^n = x^n + C_n^1 x^{n-1} y + C_n^2 x^{n-2} y^2 + \ldots + C_n^{n-1} x y^{n-1} + y^n.$$

Для большей симметрии используем такое обозначение:

$$C_{m+n}^n = \frac{(m+n)!}{n!\,m!}.$$

Теперь, благодаря полученным знаниям, мы способны определить, на какую степень простого числа p делится данный биномиальный коэффициент. Она в точности равна

$$\frac{(m+n) - \sigma_p(m+n) - \left(n - \sigma_p(n)\right) - \left(m - \sigma_p(m)\right)}{p-1} = \frac{\sigma_p(m) + \sigma_p(n) - \sigma_p(m+n)}{p-1}.$$

Красиво! Например, если $\sigma_p(m+n) = \sigma_p(m) + \sigma_p(n)$, то C_{m+n}^n на p не делится, и наоборот. Любопытно, а когда такое бывает? Ну хотя бы тогда, когда при сложении в p-ичной системе счисления чисел m и n переносов из разряда в разряд не происходит. Скажем, если сложить числа, записанные в семеричной системе счисления как 23 и 32, то получим 55 без переносов. Вывод: так как $3 + 2 \cdot 7 = 17$, $2 + 3 \cdot 7 = 23$, то C_{40}^{17} на 7 не делится.

А если перенос есть? Допустим, в каком-то i-м разряде. Скажем, у m было число $r < p$, у n — число $s < p$, а их сумма $r + s$ оказалась больше p. Тогда в следующий разряд перейдет 1, а в этом — вместо $r + s$ будет записано $r + s - p$. Тем самым в числе $m + n$ сумма цифр за счет i-го разряда будет на $p-1$ меньше, чем $\sigma_p(m) + \sigma_p(n)$. Да, как забавно — как раз на $p-1$ мы и делим. Так ведь это замечательно! Как мы сразу не догадались — верна следующая