Теорема 2. *Если p — простое число, то максимальная степень p, делящая C_{m+n}^n, равна количеству переносов при сложении чисел m и n в p-ичной системе счисления.*

Вот до какой теоремы мы добрели! Что бы извлечь из такого неочевидного факта? Глаза разбегаются. Ну давайте, простоты ради, начнем с изучения C_{2n}^n — самого большого биномиального коэффициента среди всех, входящих в разложение бинома $(x+y)^{2n}$. (Кстати, а можете ли вы доказать, что он и впрямь самый большой?) Максимальная степень p, на которую он делится, равна количеству переносов, получающихся при сложении n с самим собой в p-ичной системе счисления. Допустим, что $n < p < 2n$.

Тогда n в p-ичной системе записывается одной p-ичной «цифрой» (собственно n), а $2n$ — двумя; скажем, $2n = r + 1 \cdot p$. Это значит, что происходит ровно один перенос и, следовательно, p входит в C_{2n}^n ровно один раз. Таким образом, произведение всех простых чисел, заключенных между n и $2n$, не превосходит C_{2n}^n. Нельзя ли получить что-то поприлекательнее? Оценим C_{2n}^n грубо.

Если положить в биноме Ньютона $x = y = 1$, то получится, что

$$1 + C_{2n}^1 + C_{2n}^2 + \ldots + C_{2n}^n + \ldots + C_{2n}^{2n-1} + 1 = 2^{2n},$$

откуда

$$C_{2n}^n < 4^n.$$

Точно таким же образом произведение всех простых чисел между $n/2$ и n меньше $4^{n/2}$, между $n/4$ и $n/2$ — меньше $4^{n/4}$ и т.д. Тогда произведение всех простых чисел между 1 и n меньше

$$4^{n/2} \cdot 4^{n/4} \cdot 4^{n/8} \cdot \ldots = 4^{n/2+n/4+n/8+\ldots} < 4^n.$$

В итоге мы бесплатно получили совсем неочевидный факт:

Теорема 3. *Произведение всех простых чисел, меньших n, не превосходит 4^n.*

Упражнение 3. Докажите это строго: мы слишком небрежно делили пополам, «забыв», что бывают и нечетные числа. (Возможно, что лучший способ строгого подхода — индукция.)

Пусть теперь $p \le n$. Тогда в разложении n по крайней мере две p-ичные цифры. Если в разложении $2n$ их ровно две, то $2n < p^2$, и заведомо происходит не более одного переноса. Следовательно, верна

Лемма 1. *Если $p > \sqrt{2n}$, то максимальная степень p, делящая C_{2n}^n, не превосходит 1.*

Интересно, а когда делимости нет вообще? Так как $2n < p^2$, то $n = a_0 + a_1 p$, где $a_0 < p$, $a_1 < p/2$. Чтобы не было переносов, должно быть $a_0 < p/2$. В частности, при $a_1 = 1$ получаем, что если $a_0 = n - p < p/2$, то p не является делителем C_{2n}^n. Отсюда следует

Лемма 2. *Если $n \ge p > 2n/3$, то p не является делителем C_{2n}^n $(n > 2)$.*

Доказательство: $n < p + p/2 = 3p/2$, откуда $p > 2n/3$.

Прикинем теперь, что происходит при малых значениях $p \le \sqrt{2n}$. Там переносов уже может быть несколько, но во всяком случае не больше чем k, если $2n = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k$. Так как $2n \ge p^k$, то $\log_p 2n \ge k$, и мы можем сказать, что максимальная степень p, делящая C_{2n}^n, не превосходит $\log_p 2n$. Значит, для произвольного p справедлива

Лемма 3. *Пусть $N = p^m$ является делителем C_{2n}^n. Тогда $N \le 2n$.*

Доказательство: $p^m \le p^{\log_p 2n} = 2n$.

Ну вот, теперь мы более или менее представляем структуру числа C_{2n}^n. Его разложение на степени простых чисел состоит из трех типов сомножителей:

1) Простые числа, большие n (и, естественно, меньшие $2n$), — каждое по одному разу.

2) Простые числа, меньшие $2n/3$, но большие $\sqrt{2n}$, — каждое не более одного раза.

3) Простые числа, меньшие $\sqrt{2n}$. Тут возможна делимость на p^k с $k > 1$, но все равно полный вклад p^k каждого такого простого числа не превосходит $2n$.

Интересно, а может ли быть так, что первая группа отсутствует, т.е. между n и $2n$ нет простых чисел? Тогда все сосредоточено во второй и третьей группах. Можем ли мы оценить их реальный вклад? Произведение всех чисел второй группы, по теореме 3, не превосходит $4^{2n/3}$. Простых чисел в третьей группе заведомо меньше чем $\sqrt{2n} - 1$, так что их общий вклад, по лемме 3, не превосходит $(2n)^{\sqrt{2n}-1}$. В итоге: если между n и $2n$ нет простых чисел, то справедливо неравенство

$$C_{2n}^n < 4^{2n/3} \cdot (2n)^{\sqrt{2n}-1}. \qquad (*)$$

Какая мысль! Ведь если мы докажем, что это неравенство ложно, то одновременно докажем знаменитый постулат Бертрана: между n и $2n$ всегда имеется хотя бы одно простое число. Попробуем оценить C_{2n}^n. Коль скоро это самый большой из биномиальных коэффициентов, входящих в бином $(1+1)^{2n}$, и так как их всего там $2n + 1 < 4n$, то заведомо $C_{2n}^n > \frac{4^n}{4n}$. Из полученных неравенств следует, что

$$\frac{4^n}{4n} < 4^{2n/3} \cdot (2n)^{\sqrt{2n}-1}, \quad 4^{n/3} < 2 \cdot (2n)^{\sqrt{2n}},$$

$$\frac{n}{3} < \sqrt{2n}\log_4 2n + \frac{1}{2}, \quad \sqrt{n} < \sqrt{18}\log_4 2n + \frac{1}{2}.$$

Но хорошо известно, что логарифм — функция медленная, и $\sqrt{n}$ ее обгонит. Осталось понять, когда. Прикинем, что будет при $n = 1000$. Заведомо, $\sqrt{1000} > 30$, $\log_4 2000 < \log_4 4096 = \log_4 4^6 = 6$, т.е. $30 < \sqrt{18} \cdot 6 + \frac{1}{2}$, что неверно. Значит, при $n = 1000$ и (как вы, надеемся, легко с помощью производной докажете) для $n > 1000$ неравенство $(*)$ — ложное. Следовательно, для этих значений n справедлива

Теорема Чебышёва (постулат Бертрана). *Между n и $2n$ всегда имеется хотя бы одно простое число.*

Хорошо, а что делать с маленьким n? Там же, вроде бы, неравенство верно. Ну и бог с ним — постулат-то Бертрана тоже верен, и в этом легко убедиться, попросту просмотрев таблицу простых чисел или написав махонькую программку. Если хотите, можно и иначе — проявив больше щепетильности к оценкам, получить более точное неравенство (см., например, книгу В.Серпинского «250 задач по элементарной теории чисел»). Это уж дело вкуса.

Но, пожалуй, наша прогулка затянулась. Пора и отдохнуть, а если вы еще захотите прогуляться — для затравки несколько задачек.

1. Докажите, что для простого p и любых целых x, y число $(x+y)^p - x^p - y^p$ делится на p.

2. Обобщите предыдущую задачу на случай нескольких слагаемых и выведите отсюда малую теорему Ферма: $x^p - x$ делится на p.

3. Докажите, что если $N = p^m$, где p простое, делит биномиальный коэффициент C_n^i, то $N \le n$.

4. Докажите, что есть два простых числа между n и $2n$ для $n > 5$.

5. Докажите, что если p_k есть k-е по счету простое число, то $p_{k+2} < 2p_k$.

6. Докажите, что $n!$ не является степенью никакого числа при любом $n > 1$.