ТЕОРЕМЫ О ПРОСТЫХ ДЕЛИТЕЛЯХ

Обозначение: В данной статье речь идет только о натуральных числах. M! – M факториал.
Теорема 1. Простые делители чисел $(2^n - 1)$, при простых n, имеют вид: $An + 1$, где A – натуральное число.

Доказательство. Сравним числа $(2^n – 1)$ и $(2^f – 1)$, где $f = M!/n^t$, M – сколько угодно большое натуральное число, t – сколько угодно большое натуральное число, при котором удовлетворяется условие $(n,M!/n^t) = 1$, т.е. числа n и $M!/n^t$ взаимно простые, f – натуральное число. Т.к. M – сколько угодно большое натуральное число, то для любого простого числа p (за исключением некоторых случаев, когда $p - 1 = Bn$, т.к. f и n взаимно простые. B – натуральное число) удовлетворяется условие

$$(2^f - 1) \equiv 0 \pmod{(2^{p-1} - 1)}.$$

По Малой теореме Ферма известно, что

$$(2^{p-1} - 1) \equiv 0 \pmod{p}.$$

Следовательно, $(2^f - 1) \equiv 0 \pmod{p}$.
Нам известно, что (см. «Теоремы о взаимно простых числах» на сайте: http://logman-logman.narod.ru/) числа $(2^n - 1)$ и $(2^f - 1)$ взаимно простые, т.к. $(n,f) = 1$. Значит, любое простое число является делителем числа $(2^f - 1)$, за исключением некоторых случаев, когда $p – 1 = Bn$ и $p = Bn + 1$. Следовательно, простые делители чисел $(2^n - 1)$ имеют вид $Bn + 1$.
$Bn + 1 = An + 1$. Теорема доказана.

Теорема 2. Простые делители чисел $(S^n - 1)/(S – 1)$, при простых n, имеют вид: $(Tn + 1)$, и для ограниченного количества значений n при S = constant числа $(S^n - 1)/(S – 1)$ могут иметь простые делители d, где T – натуральное число, d – делитель числа $(S – 1)$.

Доказательство. «Теорему 2» докажем тем же путем, как доказывали «теорему 1». Сравним числа $(S^n - 1)/(S – 1)$ и $(S^f - 1)/(S – 1)$, где $f = M!/n^t$, M – сколько угодно большое натуральное число, t – сколько угодно большое натуральное число, при котором удовлетворяется условие $(n,M!/n^t) = 1$, т.е. числа n и $M!/n^t$ взаимно простые, f – натуральное число:

а) Получаем результат, как в «теореме 1», т.е. простые делители чисел $(S^n - 1)/(S – 1)$ имеют вид – $(Tn + 1)$. Кроме того

б) Т.к. в знаменателе числа $(S^f - 1)/(S – 1)$ имеется число $(S – 1)$ есть случаи, когда число $(S^f - 1)/(S – 1)$ не имеет простого делителя d, который является простым делителем числа $(S – 1)$. По этой причине можно предположить, что такие числа, как число d могут оказаться простыми делителями чисел $(S^n - 1)/(S – 1)$. Такие случаи имеются. Например:

$$(10^3 - 1)/(10 – 1) \equiv 0 \pmod{3}$$

При этом очевидно, что количество значений n с верху ограничено количеством простых делителей числа $(S – 1)$.
Теорема доказана.