Number Theory

Task 9.1

$1495 = 5 \cdot 13 \cdot 23$
$3156^{792} \equiv (3156^4)^{198} \equiv 1 \pmod 5$
$3156^{792} \equiv (3156^{12})^{66} \equiv 1 \pmod{13}$
$3156^{792} \equiv (3156^{22})^{36} \equiv 1 \pmod{23}$
Эти выводы сделаны по малой теореме Ферма для простых чисел 5, 13, 23.
По китайской теореме об остатках (далее КТО):
$3156^{792} \equiv 1$ (mod 5 * 13 * 23 = 1495)

Task 9.2

а)$x^2 \equiv x^2$ (mod p)
$x^2 \equiv x^2 - 2px + p^2$ (mod p)
$x^2 \equiv (p - x)^2$ (mod p)
Таким образом количество квадратичных вычетов <= $\frac{p-1}{2}$
Возьмем числа x $\neq$ y из $\{1, ..., \frac{p-1}{2}\}$, докажем, что невозможно $x^2 \equiv y^2$(mod p)
$(x - y)(x + y) \equiv 0$ (mod p)
|x - y| < p, x + y < p => (x - y)(x + y) не кратно p => среди чисел 1 ... p - 1 находится $\frac{p-1}{2}$ квадратичных вычетов
б) Для 17: $\frac{17-1}{2} = 8$ квадратичных вычетов

Task 9.3

Рассмотрим числа $2^n - 1, 2^n, 2^n + 1$. Среди 3 последовательных чисел долнжо быть хотя бы 1 кратное 3, но так как $2^n - 1$ и $2^n + 1$ простые, то 2^n кратно 3, что невозможно

Task 9.4

Пусть n > m:
$(2^n - 1, 2^m - 1) = (2^n - 2^m + 2^m - 1, 2^m - 1) = (2^n - 2^m, 2^m - 1)$
$(2^m(2^{n-m} - 1), 2^m - 1) = ((2^m - 1)(2^{n-m} - 1) + 1 \cdot (2^{n-m} - 1), 2^m - 1)$
$(2^{n-m} - 1, 2^m - 1)$
Повторяя аналогичные действия до конца (они ведь закончатся?...(Да, закончатся)) понимаем, что выполняется алгоритм Евклида для степеней =>
$(2^n - 1, 2^m - 1) = 2^{(n,m)} - 1$

Task 9.5

$S = n^2 + (n+1)^2 + (n+2)^2 + (n+3)^2 + (n+4)^2$

$S = n^2 + n^2 + 2n + 1 + n^2 + 4n + 4 + n^2 + 6n + 9 + n^2 + 8n + 16$

$S = 5n^2 + 20n + 30 = 5(n^2 + 4n + 6)$

То есть, если S квадрат некоего целого числа и кратно 5, то S кратно и 25. Таким образом $n^2 + 4n + 6$ кратно 5.

Проверим, возможно ли такое. Так как остатки образуют цикл, проверим для $n \equiv 0, 1, 2, 3, 4 \pmod 5$:

$n \equiv 0 \pmod 5$ => $n^2 + 4n + 6 \equiv 0 + 0 + 6 \equiv 1 \pmod 5$

$n \equiv 1 \pmod 5$ => $n^2 + 4n + 6 \equiv 1 + 4 + 6 \equiv 1 \pmod 5$

$n \equiv 2 \pmod 5$ => $n^2 + 4n + 6 \equiv 4 + 8 + 6 \equiv 3 \pmod 5$

$n \equiv 3 \pmod 5$ => $n^2 + 4n + 6 \equiv 9 + 12 + 6 \equiv 2 \pmod 5$

$n \equiv 4 \pmod 5$ => $n^2 + 4n + 6 \equiv 16 + 16 + 6 \equiv 3 \pmod 5$

Таким образом S не может быть кратно 25, то есть S не квадрат

Task 9.8 (ура, ура)

По малой теореме Ферма $1^{p-1}, 2^{p-1} ... (p-1)^{p-1}$ сравнимы с 1 по mod p. Таким образом многочлен $x^{p-1} - 1$ имеет ровно p - 1 решение в Z_p. Значит имеет место тождество: $x^{p-1} - 1 \equiv (x-1)(x-2)...(x-(p-1))$ (mod p) В частности:

$-1 \equiv (-1)(-2)...(-p+1)$ (mod p)

Если p = 2: (2 - 1)! + 1 = 2 $\equiv 0 \pmod 2$

В иных случаях p нечетное, тогда: $-1 \equiv 1 \cdot 2 ... (p-1) = (p-1)!$ (mod p)

$(p-1)! + 1 \equiv 0$ (mod p)