Kontest 2

12 czerwca 2018

1 Zasady

1. Można korzystać z dowolnych materiałów.
2. Kod ma być napisany samodzielnie tzn. 'kopiuj-wklej' jest niedozwolone, ale 'przepisz' już jest.

2 Wskazówki

1. Rozwiązania nie powinny zająć więcej niż 60*2 linii (nie wliczając debuga).
2. Przekierowywanie wejścia, wyjścia z pliku.

3 Zadania cz. II

3.1 Wielkie Twierdzenie Fermata

3.1.1 Twierdzenia

Lemat 1

$$p \in \mathbb{P} \implies \forall_{(a \mod p) \notin \{0,1\}, b, c} (a^b \equiv a^c \pmod{p} \iff b \equiv c \pmod{(p-1)})$$

Twierdzenie 1 (Wielkie Twierdzenie Fermata)
$n > 2 \implies \neg\exists_{0<a,b,c} a^n + b^n = c^n$

3.1.2 Właściwe zadanie

Niech $k = 40097, m = 1000, p = 10^9 + 7 \in \mathbb{P}$.
Niech $a, b, c \in \{k, k+1, k+2, \dots k+m\}$
Należy wypisać jakąkolwiek krotkę (a, b, c) taką, że:

$$a^{pk} + b^{pm} \equiv c^{p^2} \pmod{p}$$

lub 'NIE', jeśli taka krotka nie istnieje.

Stopnie rozwiązania zadania:

1. Pokazanie, że $\forall_k pk \equiv k \pmod{p-1}$, oraz że $p^2 \equiv 1 \pmod{p-1}$
2. Pokazanie, że wystarczy sprawdzać $a^k + b^m \equiv c \pmod{p}$
3. $O(m^3 p)$
4. $O(m^3 log(p))$
5. $O(m^2 log(m) + mlog(p))$
6. ** Pokazanie, że gdyby zamiast c^{p^2}, wziąć c^{p^2-1} i założyć, że:

$$k \equiv m \pmod{p-1},$$

   (tj. $a^m + b^m \equiv 1 \pmod{p}$) to istnieje algorytm sprawdzający istnienie krotki w $O(mlog(m))$.

Odpowiedzi: $([a, a^k \pmod{p}], [b, b^m \pmod{p}], [c, c])$
([40723,675698371],[40482,675739095],[40724,40724])
([40931,18032244],[41018,18072866],[40622,40622])