문제

환상의 나라 디디랜드에서는 인연의 증표로 끈을 하나씩 가지고 있다. 그들은 지극히 평범한 방법으로 이 끈을 이용하여 어떤 두 사람이 환상의 짝꿍인지 판단하는데, 두 사람의 끈을 서로 이어붙이고 그 끈을 다시 길이가 소수인 끈 두개로 정확히 나눌 수 있다면 두 사람은 환상의 짝꿍이라고 한다. 하지만 그들은 길이가 소수인 두개의 끈으로 나눌 수 있는지 판단하는 것이 어려워서 대부분 서로가 인연임을 모르고 그냥 지나간다고 한다. 애석하게도...

그런 그들을 위해서 어떤 두 사람이 환상의 짝꿍인지 판단하는 프로그램을 작성하라.

편의상 두 사람의 끈을 이어붙일 때와 나눌 때 손실되는 끈의 길이는 0이라고 가정한다.

입력

첫째 줄에 테스트 케이스의 수 T(1 ≤ T ≤ 500)가 주어진다.

둘째 줄부터 T개 줄에 두 사람이 가지고 있는 끈의 길이를 나타내는 정수 A, B가 공백으로 구분되어 주어진다. ($1 \le A, B \le 2 \times 10^{12}$)

출력

각 테스트 케이스마다 한 줄씩 두 사람의 끈을 이어붙이고 그 끈을 다시 길이가 소수인 두개의 끈으로 정확히 나눌 수 있다면 YES, 불가능하면 NO를 출력하라.

예제 입력 1 복사

(α) 하나의 소수가 정해지면 다른 하나는 C − α (β)

```
2
3 4
3 5
```

→ 3+4 = 7 (2 5)

→ 3+5=8 (3 5)

예제 출력 1 복사

3/5

```
YES
YES
```

① A+B 한 값을 C 라 했을 때.. α (소수)를 증가시키면서 β가 소수인지 판별한다. α가 C를 넘으면 break.

---- 시간초과.

시간을 줄일 수 있는 방법?

② i) 4 이상의 짝수는 2개의 소수로 나눌 수 있다.

ii) 2를 제외한 모든 소수는 홀수이다.

따라서 소수+2 로 만들 수 없는 모든 홀수는 2개의 소수의 합으로 나눌 수 없다.

→ 4 이상의 짝수면 YES, 홀수면 −2한 값이 소수면 YES, 나머지는 NO 이다.

밀러-라빈 소수 판별법 (Miller-Rabin Primality Test)

Posted on 2018년 6월 29일

밀러-라빈 소수 판별법은 어떤 **홀수** n이 소수인지 **확률적으로** 판별해주는 알고리즘입니다. 여기서 확률적이라는 것은, 이 알고리즘은 주어진 n이 "합성수이다" 또는 "아마도 소수일 것이다"는 대답을 내놓는다는 뜻입니다. 그러므로 이 알고리즘은 합성수를 소수라고 잘못 판별할 수 있습니다.

n이 홀수라고 했으니 $n-1$은 짝수이고, 따라서 적당한 홀수 d와 정수 s가 존재하여 $n-1 = d \cdot 2^s$입니다. 만약 n이 소수라면, n보다 작은 양의 정수 a에 대해 다음 중 하나가 성립합니다.

1. $a^d \equiv 1 \pmod{n}$
2. $r = 0, 1, 2, \cdots, s-1$중 적어도 하나에 대해 $a^{d \cdot 2^r} \equiv -1 \pmod{n}$

증명) 먼저 보조정리 하나를 증명하겠습니다.

보조정리) 소수 p에 대해 $x^2 \equiv 1 \pmod{p}$이면 $x \equiv 1 \pmod{p}$이거나 $x \equiv -1 \pmod{p}$이다.
증명) 합동식의 정의에서 $x^2 - 1 = (x+1)(x-1)$은 p의 배수이고, 따라서 $x+1$과 $x-1$ 둘 중 하나는 p의 배수여야 합니다.

페르마의 소정리에 의해서 $a^{n-1} = a^{d \cdot 2^r} \equiv 1 \pmod{n}$입니다. 보조정리에 의해 $a^{d \cdot 2^{r-1}} \equiv 1 \pmod{n}$이거나 $a^{d \cdot 2^{r-1}} \equiv -1 \pmod{n}$이 되겠죠. 후자가 성립하면 2가 성립하므로 증명 끝입니다. 전자가 성립할 경우 다시 보조정리에 의해 $a^{d \cdot 2^{r-2}} \equiv 1 \pmod{n}$이거나 $a^{d \cdot 2^{r-2}} \equiv -1 \pmod{n}$입니다. 또 전자가 성립하면 계속 보조정리를 써서 a^d까지 갑니다. 끝까지 갔는데도 $a^d \equiv 1 \pmod{n}$이면 이번엔 1번이 성립합니다. 결국 둘 중 하나는 성립하게 되어 있습니다.

역으로 어떤 홀수 n이 n보다 작은 양의 정수 a에 대해 다음을 만족하면 n은 무조건 합성수입니다.

1. $a^d \not\equiv 1 \pmod{n}$
2. $r = 0, 1, 2 \cdots, s-1$ 모두에 대해 $a^{d \cdot 2^r} \not\equiv -1 \pmod{n}$

따라서 적당히 a를 하나 고르고, 위 조건이 성립하면 n이 합성수라고 답하고, 성립하지 않으면 n은 **아마도 소수**(probable prime)라고 답합니다. 합성수를 소수라고 잘못 판별할 확률을 줄이고 싶다면, 최대한 많이 a의 값을 바꿔가며 시험해보면 됩니다. 아, 물론 $a = 1$이면 1번 조건이 항상 거짓이므로 아무런 도움이 안 됩니다…

$n = 221$로 예를 들어보겠습니다. $n - 1 = 55 \cdot 2^2$이므로 $d = 55$, $s = 2$입니다. 첫 번째로 $a = 174$를 선택해봅시다.

1. $a^d = 174^{55} \equiv 47 \not\equiv 1 \pmod{221}$
2. $a^{d \cdot 2^0} = 174^{55} \equiv 47 \not\equiv -1 \pmod{221}$,
   $a^{d \cdot 2^1} = 174^{110} \equiv -1 \pmod{221}$

2번이 성립하지 않으므로 221은 아마도 소수입니다. 두 번째로 $a = 137$을 선택해봅시다.

1. $a^d = 137^{55} \equiv 188 \not\equiv 1 \pmod{221}$
2. $a^{d \cdot 2^0} = 137^{55} \equiv 188 \not\equiv -1 \pmod{221}$,
   $a^{d \cdot 2^1} = 137^{110} \equiv 205 \not\equiv -1 \pmod{221}$

1번과 2번 모두 성립하므로 221은 소수가 아닙니다.

결국 a를 많이 넣어보지 않으면 높은 확률로 틀린다는 건데, n이 작으면 a를 이 정도만 넣어봐도 충분하다고 계산해놓은 게 있습니다. n이 2^{32} 보다 작은 합성수이면(`unsigned int`에 저장 가능한 정수라면) a에 2, 7, 61만 넣어봐도 소수로 잘못 판별되는 일이 없다고 합니다. 또, n이 2^{64} 보다 작은 합성수이면(`unsigned long long`) a에 2, 325, 9375, 28178, 450775, 9780504, 1795265022만 넣어봐도 충분합니다.