

Prob. 3 of Proc. Prob. II

Last digit of 4^{100} ?

method 1: we want $4^{100} \equiv x \pmod{10}$, with $0 \leq x \leq 9$.

mod 10

$4^0 \equiv 1$	$\downarrow \times 4$
$4^1 \equiv 4$	$\downarrow \times 4$
$4^2 \equiv 6 \equiv -4$	$\downarrow \times 4$
$4^3 \equiv 4$	\downarrow
$4^4 \equiv 6$	\downarrow
$4^5 \equiv 4$	\downarrow
$4^6 \equiv 6$	\downarrow
$4^7 \equiv 4$	\downarrow
$4^8 \equiv 6$	\downarrow
$4^9 \equiv 4$	\downarrow

\Rightarrow powers of 4 have last digit 4 if exponent is odd and have last digit 6 if exp. is even.

\downarrow 100 even
 $4^{100} \equiv 6 \pmod{10}$ \square

method 2: we want $4^{100} \equiv x \pmod{2}$ AND $4^{100} \equiv y \pmod{5}$ (\Rightarrow will tell us value mod 10)

1st: $4^{100} \equiv 0 \pmod{2}$

2nd: $4^{100} \equiv ? \pmod{5}$

\downarrow $(-1)^{100} \equiv 1 \pmod{5}$

$4^{100} \equiv (4^4)^{25} \equiv 1^{25} \equiv 1 \pmod{5}$

$a^p \equiv a \pmod{p}$, in addition if $a \not\equiv 0 \pmod{p}$ if p prime $a^{p-1} \equiv 1 \pmod{p}$.

$a^5 \equiv a$, also if $5 \nmid a$, $a^4 \equiv 1$.

$a^5 \equiv a$
 $a^4 \equiv 1$
 $a^4 = 1$

\Rightarrow the only $\equiv 1 \pmod{5}$ between 1 and 10 are 1, 6

\Rightarrow $4^{100} \equiv 6 \pmod{10}$ \square
 multi because

Prob. 2 in Proc. Prob. II: (a) Show $3 \nmid 4^{100}$.

Solⁿ: Opt. 1 is directly $4^{100} = 2^{200}$, only 2's in prime dec., so done.

\hookrightarrow Opt. 2: work modulo 3 and show $4^{100} \not\equiv 0 \pmod{3}$.

Indeed, $4^{100} \equiv 1^{100} \equiv 1 \not\equiv 0 \pmod{3}$, so done. \square

Prob. 5 Pract. Prob. I: \exists infinitely many primes of the form $6k+5$.

Solⁿ: By contradiction, assume \exists only FINITELY MANY primes of the form $6k+5$.

Call these $\{p_1, p_2, \dots, p_N\}$. Now consider the number

$$S := 6(p_1 p_2 \dots p_N) - 1, \text{ which is of the form } 6k+5 \text{ by constr.}$$

Now, $S \neq p_i$ because $S > p_i$. So S is not a prime of the form $6k+5$.

Since S is divisible by primes, we will reach a contradiction if:

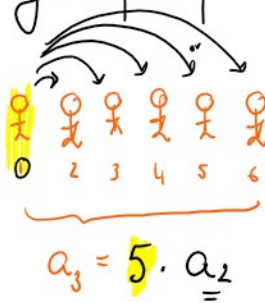
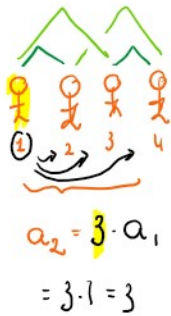
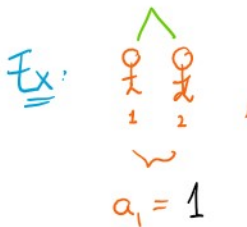
- contradiction } m {
- (1) $p_i \nmid S, 1 \leq i \leq N$: why? if $p_i \mid S$ then $p_i \mid -1$ as $p_i \mid 6(p_1, \dots, p_N)$, so it cannot be.
 - (2) S must be divided by p_i : why? S has a prime dec., primes must be $6k+1$ or $6k-1$.

If all divisors of S were $6k+1$, then S would be $6k+1$, but S is $6k-1$,

so \exists a prime of the form $6k-1$ dividing it. \blacksquare

Prob. 1 of Pset 3

$a_n := \#$ ways to pair up $2n$ players.



$$a_n = (2n-1) \cdot a_{n-1}$$

Prob. 4.(b) Show $5 \mid M^n - 6, \forall n \in \mathbb{N}$

Solⁿ: We want to show $M^n - 6 \equiv 0 \pmod{5}$.

Let's see $M \equiv 1 \pmod{5}$, also $6 \equiv 1 \pmod{5}$,

so $M^n - 6 \equiv 1^n - 1 \equiv 0 \pmod{5} \quad \square$