CIS 3362 8/25/23

① Extended Euclidean Alg for mod inverse

② For Fun: what's the probability 2 randomly chosen integers are relatively prime?

Motivation for EEA

$48x \equiv 13 \pmod{179}$

Can't divide!

Can multiply both sides ⇒ what's the magic #?

What value of a makes

$48a \equiv 1 \pmod{179}$ true?

$179 = 3 \times 48 + 35$
$48 = 1 \times 35 + 13$
$35 = 2 \times 13 + 9$
$13 = 1 \times 9 + 4$
$9 = 2 \times 4 + \boxed{1}$
$4 = 4 \times 1$

$13 - 1 \times 9 = 4$
$35 - 2 \times 13 = 9$
$48 - 1 \times 35 = 13$

$9 - 2 \times \boxed{4} = \boxed{1}$ never Δ
$9 - 2(13 - 1 \times 9) = 1$
$9 - 2 \times 13 + 2 \times 9 = 1$
$3 \times 9 - 2 \times 13 = 1$
$3(35 - 2 \times 13) - 2 \times 13 = 1$
$3 \times 35 - 6 \times 13 - 2 \times 13 = 1$
$3 \times 35 - 8 \times 13 = 1$
$3 \times 35 - 8(48 - 1 \times 35) = 1$
$3 \times 35 - 8 \times 48 + 8 \times 35 = 1$
$11 \times 35 - 8 \times 48 = 1$
$11(179 - 3 \times 48) - 8 \times 48 = 1$

$$11 \times 179 - \underline{33 \times 48} - \underline{8 \times 48} = 1$$

$$11 \times 179 - 41 \times 48 = 1$$

$$11 \times 179 - 41 \times 48 \equiv 1 \pmod{179}$$

$$-41 \times 48 \equiv 1 \pmod{179}$$

$$\Rightarrow$$

$$48^{-1} \equiv -41 \equiv 138 \pmod{179}$$

$$48x \equiv 13 \pmod{179}$$

$$\underline{\underline{138 \cdot 48}}x \equiv 138 \cdot 13 \pmod{179}$$

$$x \equiv 1794 \pmod{179}$$

$$\equiv 4 \pmod{179}$$

(2) Let the alphabet size by ~~168~~ 171, and an affine encryption function be

$$f(x) = (35x + 87) \mod 171$$

$$x = (35y + 87) \mod 171$$

$$\underline{\underline{35}}y = (x - 87) \mod 171$$

Goal: Find $35^{-1} \mod 171$.

$171 = 4 \times 35 + \underline{31}$

$35 = 1 \times 31 + 4$

$31 = 7 \times 4 + 3$

$4 = 1 \times 3 + \boxed{1}$

$\to 31 - 7 \times 4 = 3$

$\to 35 - 1 \times 31 = 4$

$\to 171 - 4 \times 35 = 31$

$4 - 1 \times \underline{\underline{3}} = 1$

$4 - 1(31 - 7 \times 4) = 1$

$4 - 1 \times 31 + 7 \times 4 = 1$

$8 \times \underline{4} - 1 \times 31 = 1$

$8(35 - 1 \times 31) - 1 \times 31 = 1$

$8 \times 35 - 8 \times 31 - 1 \times 31 = 1$

$8 \times 35 - 9 \times \underline{31} = 1$

$8 \times 35 - 9(171 - 4 \times 35) = 1$

$8 \times \underline{35} - 9 \times 171 + 36 \times \underline{35} = 1$

$\boxed{44 \times 35 - 9 \times 171 = 1}$

$44 \times 35 - 9 \times 171 \equiv 1 \pmod{171}$

$44 \times 35 \equiv 1 \pmod{171}$

$\boxed{35^{-1} \equiv 44 \pmod{171}}$

Problem: Pick 2 random ints a, b
what's probability that $\gcd(a,b)=1$?

Python → big ints
gcd function
gen ran int (nD ⇐ num digits)
list append nD digits

Golden ratio $\phi = \frac{1+\sqrt{5}}{2}$, $\frac{1}{\phi} = \frac{2}{1+\sqrt{5}} \approx .618$

Theoretical ans $= \frac{6}{\pi^2}$

Sketch $(1-\frac{1}{4})(1-\frac{1}{9})(1-\frac{1}{25})\cdots$

	a	b	
$2 \mid a$	$\frac{1}{2}$	$\frac{1}{2}$	$2 \mid a \wedge 2 \mid b$ $\frac{1}{4}$
$3 \mid a$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{9}$

⇓

$$\left(1+\frac{1}{2^2}+\frac{1}{2^4}+\frac{1}{2^6}+\frac{1}{2^8}\cdots\right)\left(1+\frac{1}{3^2}+\frac{1}{3^4}+\frac{1}{3^6}+\cdots\right)$$

$$\frac{1}{1-\frac{1}{2^2}} \times \frac{1}{1-\frac{1}{3^2}}$$

$= \frac{\pi^2}{6}$

Better Sketch of solution

Probability prime $p | a \wedge p | b$ is $\frac{1}{p^2}$

Probability either $p \nmid a \vee p \nmid b$ is $\left(1 - \frac{1}{p^2}\right)$

Since each prime is independent in this regard, probability **NO** prime $p | a \wedge p | b$ is

$$\prod_{p \in \text{Primes}} \left(1 - \frac{1}{p^2}\right)$$

Recall that $\dfrac{1}{1 - \frac{1}{p^2}} = 1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \cdots$

RHS is infinite geo series w/common ratio $\frac{1}{p^2}$.

It follows that our desired probability is

$$\prod_{p \in \text{Primes}} \left(1 - \frac{1}{p^2}\right) = \prod_{p \in \text{Primes}} \frac{1}{\sum_{i=0}^{\infty} \frac{1}{p^{2i}}}$$

Thus, we seek to find $\displaystyle\prod_{p \in \text{Primes}} \left(\sum_{i=0}^{\infty} \frac{1}{p^{2i}} \right)$.

Expand:

$$\left(1+\frac{1}{2^2}+\frac{1}{2^4}+\frac{1}{2^6}+\cdots\right)\left(1+\frac{1}{3^2}+\frac{1}{3^4}+\frac{1}{3^6}+\cdots\right)\left(1+\frac{1}{5^2}+\frac{1}{5^4}+\cdots\right)\left(1+\frac{1}{7^2}+\frac{1}{7^4}+\cdots\right)$$

Imagine each term in this expansion.
For each choice of term from every poly, for example what is circled, we ~~can~~ get a term →
in this example $\frac{1}{2^4\cdot 3^2\cdot 7^2} = \frac{1}{(2^2\cdot 3\cdot 7)^2} = \frac{1}{84^2}$

There is a one-to-one correspondence between each possible way of cirling terms (ie the terms in the expansion) and the positive integers.

Thus,

$$\prod_{p\in \text{Primes}} \left(\sum_{i=0}^{\infty} \frac{1}{p^{2i}}\right) = \sum_{i=1}^{\infty} \frac{1}{i^2}$$

and the answer to our problem is

$$\frac{1}{\sum_{i=1}^{\infty} \frac{1}{i^2}}.$$

In 1734, Euler solved $\sum_{i=1}^{\infty} \frac{1}{i^2}$, which is known as the Basel Problem.

Euler showed that $\sum_{i=1}^{\infty} \frac{1}{i^2} = \frac{\pi^2}{6}$. Incidentally $\sum_{i=1}^{\infty} \frac{1}{i^4} = \frac{\pi^4}{90}$.