Disc 2b

↳ Modular Math

↳ allows definition of finite space for nums → calculations become simple → important for polynomials → Comp → mod 2

Course ↳ intuition ↳ free points

Logistics ↳ as is disc

Mod Basics

↳ x mod m ⇒ [x = am + r] ← r

↳ remainder ← a

12 mod 5 → 2

12 = [2·5] + 2

Ex ↳ 12 mod 5 ↳ 5·2 = 10, 12 − 10 = 2

12 ≡ 2 mod 5

Congruence ↳ defines pseudo equality under mod

Math ↳ mod works for (+ − ×) exponents ① perform operation ⓪ Simplify term

holds as expected

[12 + 3] mod 5 → 5 mods = 0

exponents

Inverses

↳ a x ≡ 1 mod m

inverse of x is a

a division operation [y / x] mod m

no frac!

(ay) mod m

[1/x = a] inverse of x mod m

[a x ≡ 1 mod m]

[a · x remainder 1 with m]

Bijections → f : A → A

A ↳ finite

Set of values under mod m ⑤ ↳ {1, 2, 3, 4, 0}

f : z x ≡ y (mod m) or 5

congruence = zx → y A

find inverse of z

[z = 12] [m = 15]

A

x: 1, 2, ..., 15

y: 12, 9, 6, 3, 0, 12, 9, ...

multiple maps → 3

⊆ A

no 1

[a z ≡ 1 mod m]

↳ 3 1 in range

⇒ [12 no inverse under mod 15]

↳ 12 and 15

gcd(12, 15) ≠ 1

↳ 3

12·1 → multiple of 3 12

12·2 24

a·15 + r = 24 ↳ 24 − a·15

multiple 3 | multiple of 3

CS 70 Discrete Mathematics and Probability Theory
Summer 2021 DIS 2B

1 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of** a **modulo** m.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 10?

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3+14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

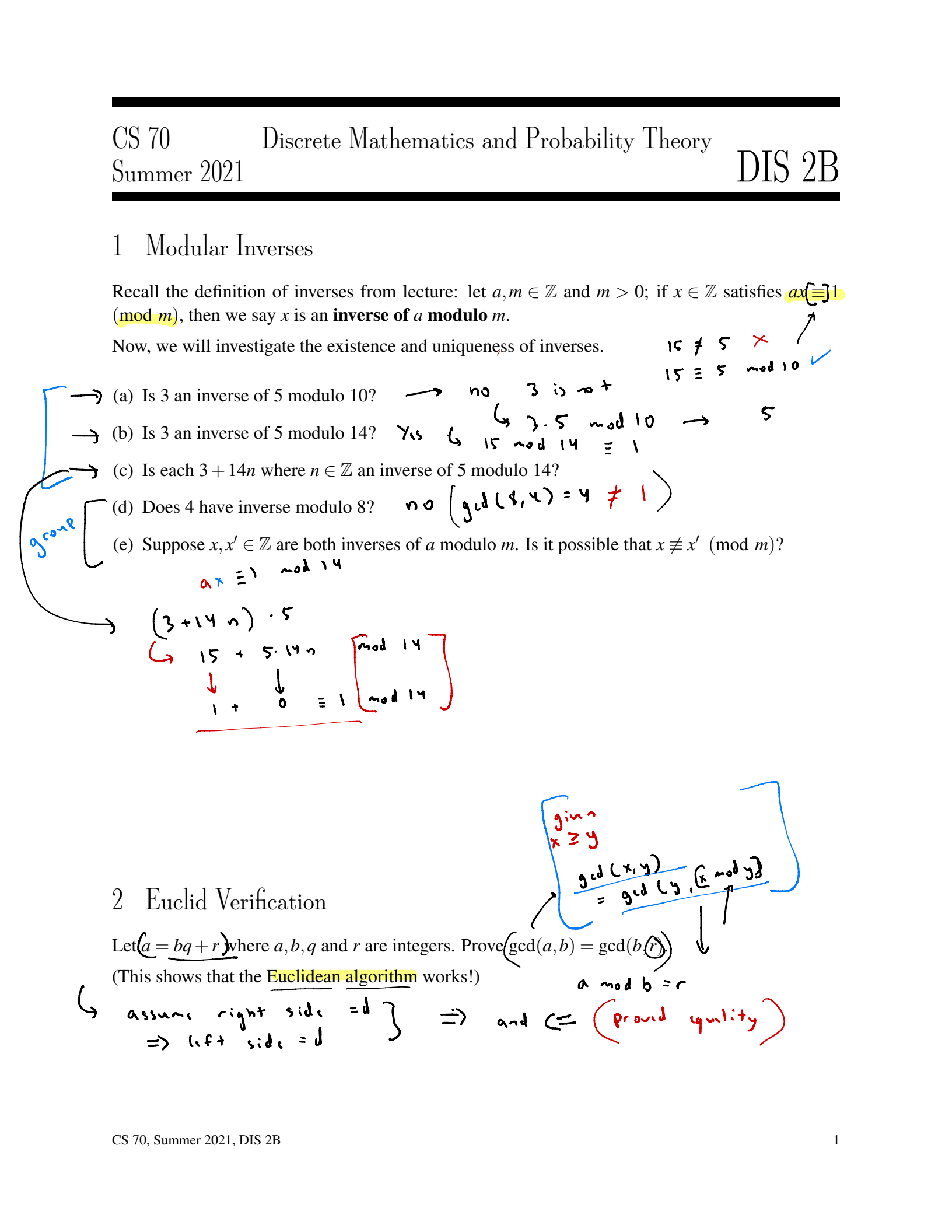
(d) Does 4 have inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

2 Euclid Verification

Let $a = bq + r$ where a, b, q and r are integers. Prove $\gcd(a,b) = \gcd(b,r)$.

(This shows that the Euclidean algorithm works!)



3 Extended Euclid

In this problem we will consider the extended Euclid's algorithm. The bolded numbers below keep track of which numbers appeared as inputs to the gcd call. Remember that we are interested in writing the GCD as a linear combination of the original inputs, so we don't want to accidentally simplify the expressions and eliminate the inputs.

(a) Note that x mod y, by definition, is always x minus a multiple of y. So, in the execution of Euclid's algorithm, each newly introduced value can always be expressed as a "combination" of the previous two, like so:

$$\begin{aligned}
\gcd(2328, 440) &= \gcd(440, 128) && [\mathbf{128} = 1 \times \mathbf{2328} + (-5) \times \mathbf{440}] \\
&= \gcd(128, 56) && [\mathbf{56} = 1 \times \mathbf{440} + ____ \times \mathbf{128}] \\
&= \gcd(56, 16) && [\mathbf{16} = 1 \times \mathbf{128} + ____ \times \mathbf{56}] \\
&= \gcd(16, 8) && [\mathbf{8} = 1 \times \mathbf{56} + ____ \times \mathbf{16}] \\
&= \gcd(8, 0) && [\mathbf{0} = 1 \times \mathbf{16} + (-2) \times \mathbf{8}] \\
&= 8.
\end{aligned}$$

(Fill in the blanks)

(b) Recall that our goal is to fill out the blanks in

$$8 = \_\_\_\_ \times \mathbf{2328} + \_\_\_\_ \times \mathbf{440}.$$

To do so, we work back up from the bottom, and express the gcd above as a combination of the two arguments on each of the previous lines:

$$\begin{aligned}
8 &= 1 \times \mathbf{8} + 1 \times \mathbf{0} = 1 \times \mathbf{8} + (1 \times \mathbf{16} + (-2) \times \mathbf{8}) \\
&= 1 \times \mathbf{16} - 1 \times \mathbf{8} \\
&= ____ \times \mathbf{56} + ____ \times \mathbf{16}
\end{aligned}$$

[*Hint*: Remember, $\mathbf{8} = 1 \times \mathbf{56} + (-3) \times \mathbf{16}$. Substitute this into the above line.]

$$= \_\_\_\_ \times \mathbf{128} + \_\_\_\_ \times \mathbf{56}$$

[*Hint*: Remember, $\mathbf{16} = 1 \times \mathbf{128} + (-2) \times \mathbf{56}$.]

$$\begin{aligned}
&= ____ \times \mathbf{440} + ____ \times \mathbf{128} \\
&= ____ \times \mathbf{2328} + ____ \times \mathbf{440}
\end{aligned}$$

(c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?

d) by contra

↳ (∃ a ∈ ℤ assume inverse of 4 mod 8)

⇒ [4a ≡ 1 (mod 8)]

⇒ 8 | 4a − 1 → [4a − 1 ≡ 0]

⇒ [4a − 1 = 8b] a, b ∈ ℤ

$\left[\frac{a-1}{2} = 2b \quad \frac{a-\frac{1}{2}}{} \not\in 2b\right]$ b int contra

↳ gcd = 1

e) (no) $\underline{x}a \equiv \underline{x'}a \equiv 1 \mod m$

we of a

↳ $xa - x'a \equiv 0$

$a(x - x') \equiv 0$

$[x\,a](x - x') \equiv 0$

(1) ⇒ $[x \equiv x' \mod m]$

↳ inverse is unique under mod m

Assume d is a divisor of [a and b] [d divides r and b]

not gcd

↳ ⇒ a − bq = r → groups d

groups of d

a and b

a mod b [a = bq + r]

↳ a and b also a divisor of r

gcd (a, b)

↳ product of all divisor

↳ 6 → 3 | 2 | 1

d d ∀d