MATH 312 MIDTERM ANSWER KEY

OCTOBER 2012

1 a) Any odd integer can be written as $(2m+1)$ for some $m \in \mathbb{Z}$.

Then $(2m+1)^2 = 4m^2 + 4m + 1$

$= 4m(m+1) + 1$.

Either m or $(m+1)$ is even.

If m is even, then let $m = 2n$ for some $n \in \mathbb{Z}$. We get $(2m+1)^2 = 4m(m+1) + 1$

$= 4(2n)(m+1) + 1$

$= 8\underbrace{n(m+1)}_{k \in \mathbb{Z}} + 1$

If $(m+1)$ is even, then let $(m+1) = 2n$ for some $n \in \mathbb{Z}$. Then $(2m+1)^2 = 4m(m+1) + 1$

$= 4m(2n) + 1$

$= 8\underbrace{mn}_{k \in \mathbb{Z}} + 1$

1b) $6 = 2 \cdot 3$

$= (1+\sqrt{-5})(1-\sqrt{-5}) \quad \in S$

$21 = 3 \cdot 7$

$= (1+4\sqrt{-5})(1-4\sqrt{-5}) \quad \in S$

Now, by showing that $2, 3, 7, (1 \pm \sqrt{-5})$, and $(1 \pm 4\sqrt{-5})$ are primes in S, we would conclude that 6 & 21 do not have unique factorisations into primes in S.

Here is the proof that $1-\sqrt{-5}$ is a prime in [a similar proof holds for the other numbers]

Recall from Assignment 3 that for $a+b\sqrt{-5} \in$ the norm $N(a+b\sqrt{-5}) = a^2 + 5b^2 \geqslant 0$.

Thus, $N(1-\sqrt{-5}) = 1^2 + 5(-1)^2 = 6$.

Recall again from Assignment 3 that a number in S is prime if it cannot be written as a product uv $(u, v \in S)$ without either $N(u) = 1$ or $N(v) = 1$.

Also, $N(uv) = N(u)N(v)$ for any $u, v \in S$.

1 b) (cont'd)

So now let's write $(1-\sqrt{-5}) = uv$ for some $u, v \in S$.

Then $6 = N(1-\sqrt{-5}) = N(uv) = N(u)N(v)$.

As the norm function, N, takes positive integer values, we must have $N(u)N(v) = 1 \cdot 6$ or $2 \cdot 3$.

But we see that $N(a+b\sqrt{-5}) = a^2 + 5b^2 \neq 2$ or 3 for any integer values of a and b.

So either $N(u)$ or $N(v)$ must be 1

$\Rightarrow 1-\sqrt{-5}$ is prime in S.

1c) Let n be the number of chocolates in each bag and q be the number of chocolates given to each student.

Then, in the format of the Euclidean Division algorithm, we get

$$63n = 23q + r$$
$$= 23q + 7$$

as 7 chocolates were left over (i.e. the remainder) after an equal number of chocolates (q) was given to each student.

In terms of congruences modulo 23, this is

$$63n \equiv 7 \pmod{23}.$$

As 7 and 23 are both primes, $\gcd(7, 23) = 1$

So to solve for n, we can actually divide by 7 and solve

$$9n \equiv 1 \pmod{23}.$$

i.e. What is the inverse of 9 modulo 23?

[Note: Even without this shortcut, you could still solve $63n \equiv 7$, but more troublesome.]

1 c) (cont'd)

As 23 is prime, each residue class (except for zero) has a unique inverse, (*)

and $9 \cdot \underbrace{18}_{n} = 162 \equiv 1 \pmod{23}$.

So $n = 18$ chocolates in each bag.

[Alternatively, no solutions for $n < 10$]

Remarks

- You can check that $n = 18$ satisfies

$$63n \equiv 7 \pmod{23}.$$

In fact, $63(18) = 23(49) + 7$, so

$$q = 49.$$

- (*) Just to illustrate unique inverses:

$1 \cdot 1 \equiv 1$

$2 \cdot 12 = 24 \equiv 1$

$3 \cdot 8 = 24 \equiv 1$

$4 \cdot 6 = 24 \equiv 1$

$5 \cdot 14 = 70 \equiv 1$

$7 \cdot 10 = 70 \equiv 1$

$9 \cdot 18 = 162 \equiv 1$

$11 \cdot 12 = 231 \equiv 1$

$13 \cdot 16 = 208 \equiv 1$

$15 \cdot 20 = 300 \equiv 1$

$17 \cdot 19 = 323 \equiv 1$

$22 \cdot 22 = 484 \equiv 1$

(mod 23)

1c) Alternate Answer

Some people may interpret the question slightly differently, and think of "7 chocolates remaining" as a shortfall of 7 chocolates, i.e.

$$63n = 23q - 7$$

← minus instead of plus

For this interpretation, a similar method as above would yield

$n = 5$ chocolates in each bag.

(and $q = 14$ chocolates given to each student)

2a) The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be uniquely written as a product of primes in a nondecreasing order.

$$8! = 8 \cdot 7 \cdot 6 \cdots 2 \cdot 1$$
$$= 2^7 \cdot 3^2 \cdot 5 \cdot 7$$

So the prime factors of 8! are 2, 3, 5 and 7.

2b) The Prime Number Theorem implies that an asymptotic formula for the n^{th} prime is $n \log_e n$.

So the millionth prime is approximately

$$1{,}000{,}000 \ (\log_e 1{,}000{,}000)$$
$$= 10^6 \left(\frac{\log_{10} 10^6}{\log_{10} e} \right) = 10^6 \cdot \left(\frac{6}{\log_{10} e} \right)$$

But $(3.3)^2 \approx 10$. So $\log_{10} e \approx \log_{10} 3.3 \approx \frac{1}{2}$

$e \approx 2.718$.

So we get $\approx 10^6 \left(\frac{6}{\frac{1}{2}} \right) = 1.2 \times 10^7$.

2c) The highest power of 5 dividing 30! is

$$\left[\frac{30}{5}\right] + \left[\frac{30}{5^2}\right] + \left[\frac{30}{5^3}\right] + \cdots$$

$$= 6 + 1 + 0 + 0 + 0 + \cdots$$

$$= 7$$

3a) $300 = 2 \cdot (105) + 90$

$105 = 1 \cdot (90) + 15$

$90 = 6 \cdot (15) + 0$

So $\gcd(300, 105) = 15$

Then $15 = 105 - 1 \cdot (90)$

$= 105 - 1 \cdot [300 - 2(105)]$

$= 3(105) - 1 \cdot (300)$

3b)i) TRUE.

gcd(137, 119) must be odd.

gcd(256, 238) must be even.

So $(137, 119) \neq (256, 238)$.

---

b)ii) FALSE

Lamé's Theorem from the textbook states that for $0 < a < b \in \mathbb{Z}$, gcd(a, b) can be found in no more than 5n steps, where n is the number of digits in the decimal expansion of a.

Here, $a < 100 \Rightarrow n \leq 2$.

So $5n \leq 5(2) = 10$.

But "≤ 10" is not the same as

"less than 10"

i.e., it could actually be 10 steps, so the statement is false.

iii) FALSE

$$a \equiv b \pmod 7$$

$$\Downarrow$$

$$7 \mid (a-b)$$

$$\Downarrow$$

$$a-b = 7m \text{ for some } m \in \mathbb{Z}$$

$$\Downarrow$$

$$5(a-b) = 5 \cdot 7m$$

$$= 7(5m)$$

$$\Downarrow$$

$$7 \mid 5(a-b)$$

$\therefore$ 7 does divide $5(a-b)$