Warm up!

(a) Prove $n! + 3$ is not prime ($n \geq 3$).

(b) Prove that for every prime k,
We can find k consecutive non-primes.

Objectives

1) Results from Monday's survey
2) Warm-up (number theory proof)
3) Warm-up (GCD proof)
4) Motivation
5) Very fun modular arithmetic proof

Results from survey

Question 4

Is there a song or musical piece you'd like to request for before the class starts? Any language is okay, but preferably under 7 minutes and with no inappropriate lyrics.

Expand Responses

Question 5

Or maybe, you would prefer that I don't play any music at all?

True	2	(2.47 %)
False	79	(97.53 %)

Question 11

Please answer the following:

My vocal volume (1 = too loud, 10 = perfect volume)

1	0	(0 %)
2	0	(0 %)
3	2	(2.47 %)
4	0	(0 %)
5	0	(0 %)
6	1	(1.23 %)
7	1	(1.23 %)
8	3	(3.7 %)
9	16	(19.75 %)
10	58	(71.6 %)

Warm up!

(a) Prove $n! + 3$ is not prime ($n \geq 3$).

(b) Prove that for every prime k,
We can find k consecutive non-primes.

This was a MATH 135 question, from Fall 2007:

7. Suppose that p is a prime number with $p > 3$.

   (a) Prove that the remainder when p is divided by 4 is 1 or 3.

   (b) Prove that the remainder when p is divided by 6 is 1 or 5.

8. (a) Prove that if $n \geq 3$, then $n! + 3$ is not prime.

   (b) Prove that for every $k \in \mathbb{P}$, k consecutive positive integers that are not prime can be found. (A good way to prove this is to explicitly show what these k integers could be.)

Prove $n! + 3$ is not prime ($n \geq 3$).

If $n! + 3$ is not prime,
can you tell me a factor apart from 1 or itself ?

Try the smallest possible prime factor:

Does $2 \mid n! + 3$?

Prove $n! + 3$ is not prime ($n \geq 3$).

If $n! + 3$ is not prime,
can you tell me a factor apart from 1 or itself ?

Try the smallest possible prime factor:

Does $2 \mid n! + 3$? ✗ $n!$ is even, $n! + 3$ is odd!

Does $3 \mid n! + 3$?

Prove $n! + 3$ is not prime ($n \geq 3$).

If $n! + 3$ is not prime,
can you tell me a factor apart from 1 or itself ?

Try the smallest possible prime factor:

Does $2 \mid n! + 3$? ✗ $n!$ is even, $n! + 3$ is odd!

Does $3 \mid n! + 3$? ✓ $3 \mid n!$ AND $3 \mid 3 \Rightarrow 3 \mid n! + 3$

Prove that for every prime k, We can find k consecutive non-primes.

$3 \mid n! + 3$

$r \mid n! + r$

Prove that for every prime k, We can find k consecutive non-primes.

$3 \mid n! + 3 \qquad 3 \mid n!$ AND $3 \mid 3 \Rightarrow 3 \mid n! + 3$

$r \mid n! + r \qquad r \mid n!$ AND $r \mid r \Rightarrow r \mid n! + r$

k consecutive non-primes ($n = k+1$):

$(k+1)! + 2,\ (k+1)! + 3,\ (k+1)! + 4,\ \ldots,\ (k+1)! + k+1$

Prove that for every prime k,

We can find k consecutive non-primes.

$3 \mid n! + 3 \qquad 3 \mid n!$ AND $3 \mid 3 \Rightarrow 3 \mid n! + 3$

$r \mid n! + r \qquad r \mid n!$ AND $r \mid r \Rightarrow r \mid r! + r$

k consecutive **non-primes:**

$(k+1)! + 2 \, , \, (k+1)! + 3 \, , \, (k+1)! + 4 \, , \, \ldots \, , \, (k+1)! + k+1$

Divisible by r=2 Divisible by r=3 Divisible by r=k+1

Prove that for every prime k, We can find k consecutive non-primes.

k consecutive **non-primes:**

$$(k+1)! + 2\ ,\ (k+1)! + 3\ ,\ (k+1)! + 4\ ,\ \ldots\ ,\ (k+1)! + k+1$$

k = 2. Consecutive nonprimes: $3! + 2$, $3! + 3$ (**8,9**)

k = 3. Consecutive nonprimes: $4! + 2$, $4! + 3$, $4! + 4$ (**26,27,28**)

k = 5. Consecutive nonprimes: $6! + 2$, $6! + 3$, …, $6! + 6$ (**722, 723, 724, 725, 726**)

$723 = 3 \times 241$

For number theory **proofs**:

there's no step-by-step procedure that always works, like "product rule" in calculus

"O King, for traveling over the country there are royal roads and roads for common citizens; but in geometry there is one road for all"

Alexander the Great was told this when he asked Menaechmus for a shortcut to learning geometry *(circa 330 BC).*

No short-cut: practice proofs and you will get better!

Warm up!

Math 135 — Fall 2000 — Alternate Final *Page 1 of 1* REPRINTED BY MATHSOC ⋈

Instructors: R. André, S. D'Alessio, J. Geelen, J, Hooper, L. Lipták, C.T. Ng, I. VanderBurgh, S. Wolf, D. Younger

[12] 1. Solve the following system of linear congruences:

$$\begin{aligned} 3x &\equiv 10 \pmod{41} \\ x &\equiv 9 \pmod{21}. \end{aligned}$$

[5] 2. (a) Prove that $P \implies (Q \text{ OR } R)$ is logically equivalent to $(P \text{ AND } (\text{NOT } Q)) \implies R$.

[2] (b) Determine whether the following proposition is true or false:

$$\forall a, b, c\ \exists x, y\ (ax + by = c),$$

where the universe of discourse is the set of all integers. (Justify your answer.)

[8] 3. Let Let $a_1 = 2$, $a_2 = 10$, and $a_n = 7a_{n-1} - 12a_{n-2}$ for all $n \geq 3$. Prove that $a_n = 4^n - 2(3^{n-1})$ for all $n \geq 1$.

[6] 4. (a) Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{R}$. Prove that if $c \in \mathbb{C}$ is a root of $f(x)$ then $\bar{c}$ (the complex conjugate of c) is also a root of $f(x)$.

[6] (b) Factor the polynomial $f(x) = x^4 - x^3 - 11x^2 - x - 12$ in $\mathbb{R}[x]$. (Hint: i is a root of $f(x)$.)

[8] 5. Prove that if two integers a and b are coprime, then ab and $a + b$ are coprime. (Recall: a and b are *coprime* if $\text{GCD}(a, b) = 1$.)

Warm up!

Prove:

If $\gcd(a,b)=1$ then $\gcd(a+b,ab) = 1$

Strategy

Bézout Identity: Good when GCD is in hypothesis

GCD WR: Good when terms in GCD depend on each other

GCD CT: Good when GCD is in conclusion

Definition of GCD: Good when nothing else seems to work

GCDPF: Good when you're desperate

If gcd(a,b)=1 then:

$ax + by = 1$ (Bézout Identity)

$(ax)^2 + (by)^2 + 2abxy = 1$ (square both sides)

What do we need, to prove that gcd(ab,a+b)=1 ?

CCT: gcd(a+b,ab)=1 ***iff*** $(a+b)p + (ab)q = 1$

$$(a + b)(x^2a + y^2b) + ab(2xy - x^2 - y^2) = 1$$

Motivation!

We have proven:

$\gcd(22a + 7, 3a + 1) = 1$

$\gcd(a,b) = 1 \Rightarrow \gcd(ab, a+b) = 1$

$\gcd(a,b) = 1 \Rightarrow \gcd(an+u, bn+v) = 1$

$a \mid 2b + c \Rightarrow (a \nmid b - 2d) \vee (a \mid c + 4d)$

In calculus the motivation is clear:

Optimize profit based on revenue and cost functions

Rate of change:
How much deceleration,
does the self-driving car need, to stop before stop sign

Rate of change of COVID growth

Can you see why we care about whether or not:

$$a \mid 2b+\gcd(u,v) \Rightarrow (a \nmid b - 2\gcd(e,f)) \vee (a \mid \gcd(u,v) + 4\gcd(e,f)) \text{ ?}$$

When I was an undergrad,
a friend was doing a research project with title:

"Are there any odd triperfect numbers?"

Triperfect: Sum of all divisors of N is 3N.

Triperfect numbers [edit]

A number n with $\sigma(n) = 3n$ is **triperfect**. An odd triperfect number must exceed 10^{70} and have at least 12 distinct prime factors, the largest exceeding 10^5.[3]

Why do we care whether or not $n! + 3$ is prime?

Whether or not numbers with certain properties exist, is at the heart of cryptography!

If I have pictures of me that I don't want you to see, or I'm sending a private message to a family member:
I encode it with secret code,
so you have to solve a puzzle to read the message.

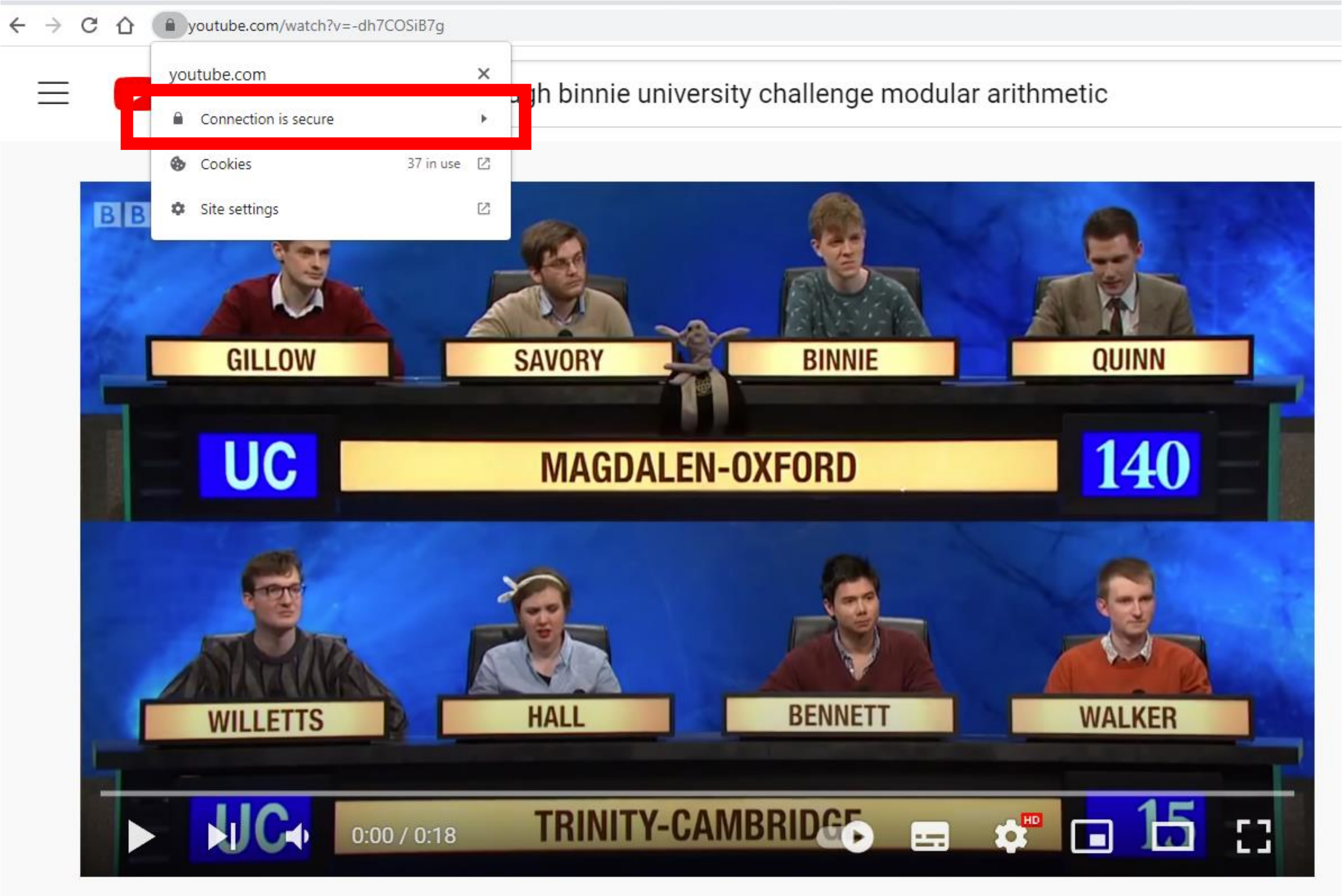
My computers have the puzzle pieces, yours don't!

Chapter 9 will be about RSA cryptography

But we have to teach you Chapter 8 first

RSA cryptography is everywhere

For example, everytime you visit Youtube



CO 485: Mathematics of Cryptography

Requires: PMATH 334, 336, 346, or 347

Requires: MATH 235

Requires: MATH 136

Requires: MATH 135

CO 487: Applied Cryptography

Requires: MATH 135 + STAT 230 or 240

CO 487 LEC 0.50

Course ID: 010136

Applied Cryptography

A broad introduction to cryptography, highlighting the major developments of the past twenty years. Symmetric ciphers, hash functions and data integrity, public-key encryption and digital signatures, key establishment, key management. Applications to Internet security, computer security, communications security, and electronic commerce. [Offered: W]

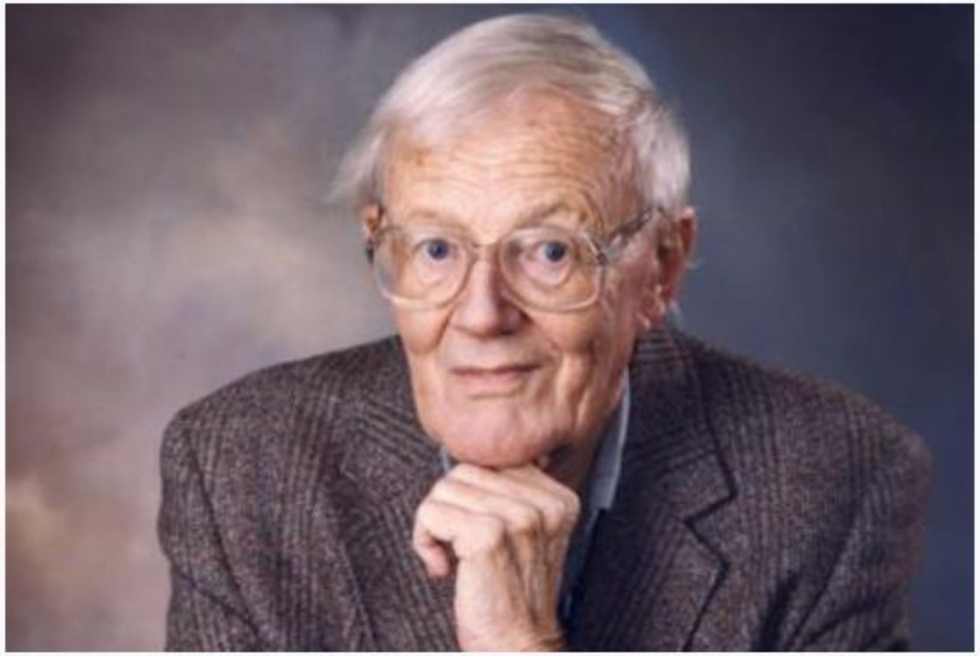
Prereq: MATH 135 or 145, STAT 206 or 220 or 230 or 240; Level at least 3A

CO 487: Applied Cryptography

Requires: MATH 135 + STAT 230 or 240

William Thomas Tutte OC FRS FRSC (/tʌt/; 14 May 1917 – 2 May 2002) was an English and Canadian codebreaker and mathematician. During the Second World War, he made a brilliant and fundamental advance in cryptanalysis of the Lorenz cipher, a major Nazi German cipher system which was used for top-secret communications within the Wehrmacht High Command. The high-level, strategic nature of the intelligence obtained from Tutte's crucial breakthrough, in the bulk decrypting of Lorenz-enciphered messages

W. T. Tutte



Born	14 May 1917 Newmarket, Suffolk, England
Died	2 May 2002 (aged 84) Kitchener, Ontario, Canada

Also, something that the course notes won't tell you,

These gcd theorems are at the heart of algorithms that allow computers to do ***FAST*** computations.

CS 487: Introduction to symbolic computation

Requires: CS 234 or CS 240

Requires: MATH 136

Requires: MATH 135

18 second video:

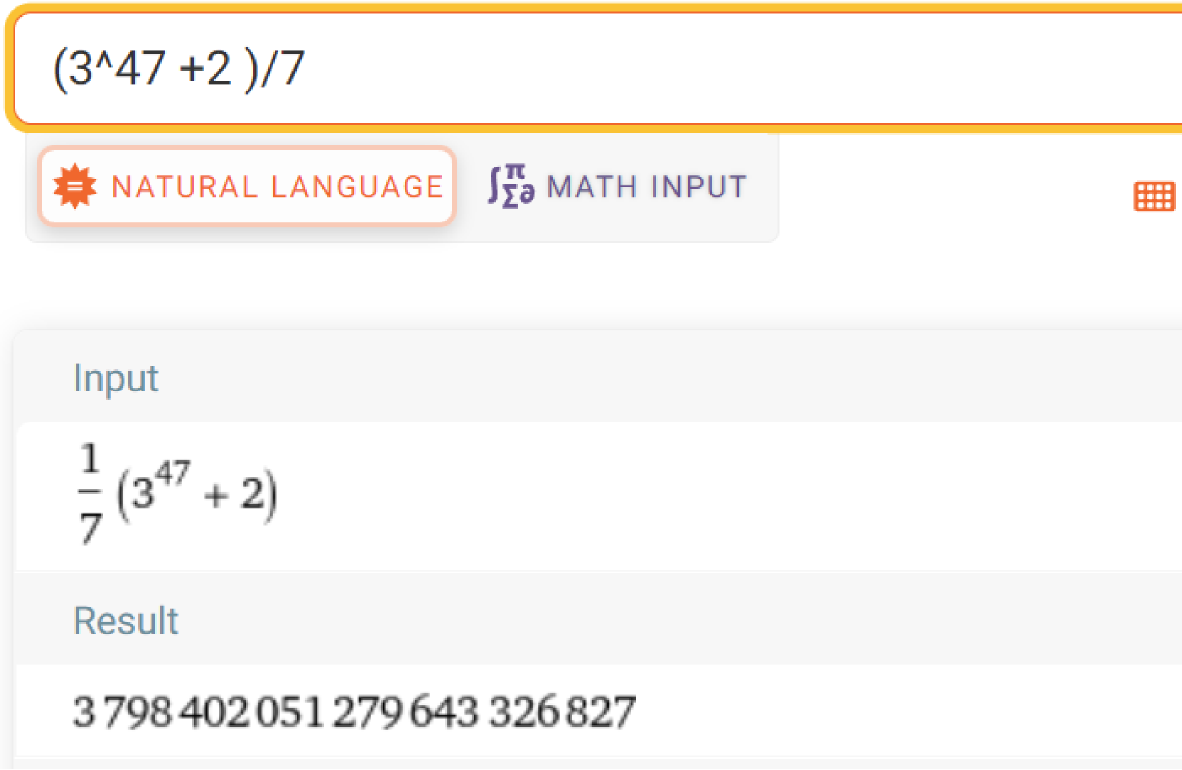
Former student of mine I taught at Oxford University

Host: How did you know that?

Hugh Binnie: “Modular arithmetic”

$$
\begin{aligned}
28 &\equiv 0 &\pmod 7\\
28 - 1 &\equiv -1 &\pmod 7\\
27 &\equiv -1 &\pmod 7
\end{aligned}
$$

$$
\begin{aligned}
3^{47} &\equiv \, ? &\pmod 7\\
&\equiv 3^2 3^{45} &\pmod 7\\
&\equiv 3^2 (3^3)^{15} &\pmod 7\\
&\equiv 9(27)^{15} &\pmod 7\\
&\equiv 2(-1)^{15} &\pmod 7\\
&\equiv -2 &\pmod 7\\
3^{47} + 2 &\equiv 0 &\pmod 7.
\end{aligned}
$$



$$7 \mid 3^{47} + 2$$

$$2^{22}3^{33}5^{55} \pmod{11}$$

Thank you!

- Wednesday 3 November:
  - Regrade requests for midterm (due 3 Nov)

- **Wednesday 3 November:**
  - **Submit Written Assignment 6: WA6**

- Thursday 4 November:
  - **Read Chapters 6.7 – 7.2 (pg. 110 – 121) and 0.5 of Polynomials**
  - **Chapter 8 (hardest chapter in MATH 135, relies on pgs. 110-121)**

- Thursday 4 November:
  - Start WA07 (covers Pages **110-121**).