Math 55: Discrete Math
GSI Charles Holton
September 17, 1997

Section	*Problems*
§2.5	2e, 2f, 8, 10, 12, 14, 15, 22, 32, 33
§2.6	5, 10, 15, 23
§3.1	3, 5, 11, 13, 15, 20, 42

(§2.5, #2) Express the greatest common divisor of each pair of integers as a linear combination of these integers.

e) $117, 213$.

$$\begin{aligned} 213 &= 1 \cdot 117 + 96 \\ 117 &= 1 \cdot 96 + 21 \\ 96 &= 4 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

so $\gcd(117, 213) = 3$. We write

$$\begin{aligned} 3 &= 12 - 1 \cdot 9 \\ &= 12 - 1 \cdot (21 - 1 \cdot 12) \\ &= 2 \cdot 12 - 1 \cdot 21 \\ &= 2 \cdot (96 - 4 \cdot 21) - 1 \cdot 21 \\ &= 2 \cdot 96 - 9 \cdot 21 \\ &= 2 \cdot 96 - 9 \cdot (117 - 1 \cdot 96) \\ &= 11 \cdot 96 - 9 \cdot 117 \\ &= 11 \cdot (213 - 1 \cdot 117) - 9 \cdot 117 \\ &= 11 \cdot 213 - 20 \cdot 117. \end{aligned}$$

f) $0, 223$. $223 = 1 \cdot 223 + 0$.

(§2.5 #8) Find an inverse of 144 modulo 233.

Applying the Euclidean algorithm (this is a worst-case) yields:

$$\begin{aligned} 233 &= 1 \cdot 144 + 89 \\ 144 &= 1 \cdot 89 + 55 \\ 89 &= 1 \cdot 55 + 34 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

so that $\gcd(144, 233) = 1$ (this is of course necessary in order that 144 have an inverse modulo 233). Write, as before

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 \\ &= 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot)8 = 5 \cdot 8 - 3 \cdot 13 \\ &= 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21) = 13 \cdot 21 - 8 \cdot 34 \\ &= 13 \cdot (55 - 1 \cdot 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\ &= 13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55) = 34 \cdot 55 - 21 \cdot 89 \\ &= 34 \cdot (144 - 1 \cdot 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89 \\ &= 34 \cdot 144 - 55 \cdot (233 - 1 \cdot 144) = 89 \cdot 144 - 55 \cdot 233 \end{aligned}$$

Thus 89 is an inverse of 144 modulo 233.

(§2.5 #10) Show that an inverse of a modulo m does not exist if $\gcd(a, m) > 1$.

We will prove the contrapositive: if a has an inverse modulo m then $\gcd(a, m) = 1$.

Let b be any inverse of a modulo m. Then $ab \equiv 1 \pmod{m}$, by definition of an inverse. This implies that $ab = nm + 1$ for some integer n, or equivalently, $ab - nm = 1$. Since every common divisor of a and m must divide $ab - nm$, this proves that $\gcd(a, m) = 1$.

(§2.5 #12) Solve the congruence $2x \equiv 7 \pmod{17}$.

It is easy to see that 9 is an inverse of 2 modulo 17 (just check: $9 \cdot 2 = 18 \equiv 1 \pmod{17}$). Thus $9 \cdot 2x \equiv 9 \cdot 7 \pmod{17}$. After simplifying we have $x \equiv 12 \pmod{17}$. The solutions are exactly the numbers $x = 12 + 17n$.

(§2.5 #14a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.

We know that each of the integers $1, 2, 3, \ldots 10$ has an inverse modulo 11 (because 11 is prime). One can easily check that the inverse of 2 is 6, the inverse of 3 is 4, the inverse of 5 is 9, and the inverse of 7 is 8.

(§2.5 #14b) Use part (a) to show that $10! \equiv -1 \pmod{11}$.

$10! = 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 \equiv -1 \pmod{11}$.

(§2.5 #15) Show that if p is prime, the only solutions of $x^2 \equiv 1 \pmod{p}$ are integers x such that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

It is clear that all integers which are congruent to $\pm 1 \pmod{p}$ are solutions of $x^2 \equiv 1 \pmod{p}$.

If $x^2 \equiv 1 \pmod{p}$ then $(x - 1)(x + 1) = x^2 - 1 \equiv 0 \pmod{p}$. Hence $p \mid (x - 1)(x + 1)$, and since p is prime, p must divide $(x - 1)$ or $(x + 1)$. But this means $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

(§2.5 #22) Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?

The integers $10+15n$ are divisible by 5 and congruent to 1 modulo 3. By the Chinese Remainder Theorem, these are the only solutions.

(§2.5 #32) Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 10.

(AT)(TA)(CK) is written as 0019 1900 0210. To encrypt we must compute $0019^{13} \equiv 2299 \pmod{2537}$, $1900^{13} \equiv 1317 \pmod{2537}$ and $0210^{13} \equiv 2117 \pmod{2537}$. The encrypted message is 2299 1317 2117.

(§2.5 #33) What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0067 1947 0671?

We must compute $0067^{937} \pmod{2537}$, $1947^{937} \pmod{2537}$ and $0671^{937} \pmod{2537}$. According to my computer we get 1808 1121 0417. Translating back to letters we get SILVER.

(§2.6 #5) Find a matrix A such that

$$\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} A = \begin{bmatrix} 3 & 0 \\ 1 & 2 \end{bmatrix}$$

Solve the system of equations:

$$2a_{11} \quad +3a_{21} = 3$$

$$\begin{aligned} 2a_{12} \quad &+3a_{22} = 0 \\ 1a_{11} \quad &+4a_{21} = 1 \\ 1a_{12} \quad &+4a_{22} = 2 \end{aligned}$$

The solution is $a_{11} = \frac{9}{5}$, $a_{12} = -\frac{6}{5}$, $a_{21} = -\frac{1}{5}$ and $a_{22} = \frac{4}{5}$. Thus,

$$A = \begin{bmatrix} 9/5 & -6/5 \\ -1/5 & 4/5 \end{bmatrix}$$

(§2.6 #10) Let A be a 3×4 matrix, B a 4×5 matrix, and C a 4×4 matrix. Determine which of the following products are defined and find the size of those that are defined.

a) AB is a 3×5 matrix.
b) BA is undefined.
c) AC is a 3×4 matrix.
d) CA is undefined.
e) BC is undefined.
f) CB is a 4×5 matrix.

(§2.6 #15) Let

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Find a formula for A^n whenever n is a positive integer.

$$A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$$

(§2.6 #23) Show that the conventional algorithm uses $m_1 m_2 m_3$ multiplications to compute the product of the $m_1 \times m_2$ matrix A and the $m_2 \times m_3$ matrix B.

The product $C = AB$ is an $m_1 \times m_3$ matrix. Each entry c_{ij} is the sum of the m_2 products $a_{ik}b_{kj}$, $k = 1, 2, \ldots m_2$. Thus there are $m_1 m_2 m_3$ multiplications required to compute C in this way.

(§3.1 #3) Determine whether each of the following arguments is valid. If an argument is correct, what rule of inference is being used? If it is not, what fallacy occurs?

a) If n is a real number such that $n > 1$, then $n^2 > 1$. Suppose that $n^2 > 1$. Then $n > 1$.

This is clearly incorrect (fallacy of confirming the conclusion).

b) The number $\log_2 3$ is irrational if it is not the ratio two integers. Therefore, since $\log_2 3$ cannot be written in the form a/b where a and b are integers, it is irrational.

The argument is incorrect (fallacy of begging the question).

c) If n is a real number with $n > 3$, then $n^2 > 9$. Suppose that $n^2 \leq 9$. Then $n \leq 3$.

The argument is valid (modus tollens).

d) A positive integer is either a perfect square or it has an even number of positive integer divisors. Suppose that n is a positive integer that has an odd number of positive integer divisors. Then n is a perfect square.

The argument is valid (disjunctive syllogism).

e) If n is a real number with $n > 2$, then $n^2 > 4$. Suppose that $n \leq 2$. Then $n^2 \leq 4$.

The argument is invalid (denying the hypothesis).

(§3.1 #5) Prove the proposition $P(0)$, where $P(n)$ is the proposition "If n is a positive integer greater than 1, then $n^2 > n$." What kind of proof did you use?

$P(0)$ is the proposition "If 0 is a positive integer greater than 1, then $0^2 > 0$." Since 0 is not a positive integer greater than 1, $P(0)$ is valid ($\neg p \wedge (p \rightarrow q)$ is always true).

(§3.1 #11) Prove that the sum of an irrational number and a rational number is irrational using a proof by contradiction.

Suppose that the statement is false. Then there exist a rational number r and an irrational number s for which $s + r$ is not irrational. This implies that $s + r$ is a rational number, so we can write $s + r = p/q$ for some integers p and q with $q \neq 0$. Since r is also rational, we can find integers a and $b \neq 0$ with $a/b = r$. Then $s = p/q - r = p/q - a/b = \frac{pb - qa}{qb}$. But both $pb - qa$ and qb are integers, and hence s is a rational number, contradicting that it should be irrational. Therefore the negation of the statement is false, so the statement must itself be true.

(§3.1 #13) Prove or disprove that the product of two irrational numbers is irrational.

Disprove by counterexample:

We have seen that $\sqrt{2}$ is irrational, yet $\sqrt{2} \cdot -\sqrt{2} = -2$ is rational. Thus the product of two irrational numbers need not be irrational.

(§3.1 #15) Prove or disprove that $n^2 - n + 41$ is prime whenever n is a positive integer.

Counterexample:

41 is a positive integer and $41^2 - 41 + 41 = 41^2$ is obviously not prime.

(§3.1 #20) Prove that the square of an integer not divisible by 5 leaves a remainder of 1 or 4 when divided by 5.

Let n be any integer not divisible by 5 and consider the possibilities for $n \pmod 5$:

If $n \equiv 1 \pmod 5$ then $n^2 \equiv 1 \pmod 5$, or equivalently, n^2 leaves a remainder of 1 when divided by 5.

If $n \equiv 2 \pmod 5$ then $n^2 \equiv 4 \pmod 5$, so that n^2 leaves a remainder of 4 when divided by 5.

If $n \equiv 3 \pmod 5$ then $n^2 \equiv 9 \equiv 4 \pmod 5$ and n^2 leaves a remainder of 4 when divided by 5.

Finally, if $n \equiv 4 \bmod 5$ then $n^2 \equiv 16 \equiv 1 \pmod 5$.

(§3.1 #42) Prove or disprove that if $p_1, p_2, \ldots, p_n$ are the n smallest primes, then $p_1 p_2 \cdots p_n + 1$ is prime.

Disprove by counterexample:

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510511 = 19 \cdot 26869$ is not prime.