c) gcd (1001, 1331) e) gcd (12345, 54321)
d) gcd (1000, 5040) f) gcd (9888, 6060)

d-n: a) By Lemma 1, gcd (12, 18) is the same as the gcd of the smaller of these 2 numbers (12)

Week 8: Homework

P-1 What are the quotient & remainder when
a) 19 is divided by 7
b) -111 is divided by 11
c) 789 is divided by 23
d) 1001 is div. by 13
e) 0 is div. by 19
f) 3 is divided by 5.
g) -1 is div by 3
h) 4 is divided by 1.

Solu-n: In each case we need to find (the unique integers) q and r such that $a = dq + r$ and $0 \le r < d$ where a and d are the given integers. In each case $q = \lfloor a/d \rfloor$

a) $19 = 7 \cdot 2 + 5$ so $q = 2$ and $r = 5$
b) $-111 = (-11)\cdot(-11) + 10$ so $q = -11$ & $r = 10$
c) $789 = 23 \cdot 34 + 7$ so $q = 34$ $r = 7$
d) $1001 = 13 \cdot 77$ $q = 77$ $r = 0$
e) $0 = 19 \cdot 0 + 0$ $q = 0$ $r = 0$
f) $3 = 5 \cdot 0$ $q = 0$ $r = 3$
g) $-1 = 3 \cdot (-1) + 2$ $q = -1$ $r = 2$
h) $4 = 1 \cdot 4 + 0$ $q = 4$ $r = 0$

P-2 Find a formula for the integer with smallest absolute value that is congruent to an integer a modulo m, where m is a positive integer.

$$f(x) = \begin{cases} x \bmod m & \text{if } x \bmod m \le \lceil m/2 \rceil \\ (x \bmod m) - m & \text{if } x \bmod m > \lceil m/2 \rceil \end{cases}$$

If m is even we can, alternatively take $f(m/2) = -m/2$

P-3: Find counterexamples to each of these statements about congruences.

a) If $ac \equiv bc \pmod m$ where a, b, c & m are integers with $m \ge 2$, then $a \equiv b \pmod m$

b) If $a \equiv b \pmod m$ ~~where a, b, c~~ & $c \equiv d \pmod m$ where a, b, c, d & m are integers with c & d positive & $m \ge 2$, then $a^c \equiv b^d \pmod m$

descent
+2 P2
1 & 3
5 P3

take
+3 P3
2 & 3
6 P3

P. Who take
1 & 2

Corollary: Let m be a positive integer & let a & b be integers. Then

1) $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

2) $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Arithmetic Modulo m

Definitions: Let $Z_m = \{0, 1, \ldots, m-1\}$

The operation $+_m$ is defined ...

This is additional ...

P-12.

Sol-n: a) To show that this conditional statement does not necessarily hold, we need to find an example in which $ac \equiv bc \pmod m$ but $a \not\equiv b \pmod m$. Let $m=4$ & $c=2$. Let $a=0$, $b=2$. Then $ac=0$ & $bc=4$ so $ac \equiv bc \pmod 4$ but $0 \not\equiv 2 \pmod 4$.

b) To show that this conditional statement does not necessarily hold, we need to find an example in which $a \equiv b \pmod m$ & $c \equiv d \pmod m$, but $a^c \not\equiv b^d \pmod m$. If we try a few randomly chosen positive integers we will soon find one. Let $m=5$, $a=3$, $b=3$, $c=1$ & $d=6$. Then $a^c=3$ & $b^d=729 \equiv 4 \pmod 5$, so $3^1 \not\equiv 3^6 \pmod 5$ even though $3 \equiv 3 \pmod 5$ & $1 \equiv 6 \pmod 5$.

P-4: Show that if a, b, k and m are integers such that $k \geq 1$, $m \geq 2$ and $a \equiv b \pmod m$, then $a^k \equiv b^k \pmod m$.

S-n: There are at least 2 ways to prove it. One way is to invoke Theorem 5 repeatedly. Since $a \equiv b \pmod m$, Theorem 5 implies that $a \cdot a \equiv b \cdot b \pmod m$ i.e. $a^2 \equiv b^2 \pmod m$. Invoking theorem 5 again, since $a \equiv b \pmod m$ & $a^2 \equiv b^2 \pmod m$ we obtain $a^3 \equiv b^3 \pmod m$. After $k-1$ applications of this process, we obtain $a^k \equiv b^k \pmod m$, as desired.

Alternatively we can argue directly, using the algebraic identity $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1})$. Specifically, the hypothesis that $a \equiv b \pmod m$ means that $m \mid (a-b)$. Therefore by theorem 1 (ii), m divides the right-hand side of this identity, so $m \mid a^k - b^k$. This means precisely that $a^k \equiv b^k \pmod m$.

P-5 Write out the additional & multiplication tables for Z_5 where by addition & multip. we mean $+_5$ & $\cdot_5$

Sol-n:

0+0=0	0+1=1	0+2=2	0+3=3	0+4=4
1+0=1	1+1=2	1+2=3	1+3=4	1+4=0
2+0=2	2+1=3	2+2=4	2+3=0	2+4=1
3+0=3	3+1=4	3+2=0	3+3=1	3+4=2
4+0=4	4+1=0	4+2=1	4+3=2	4+4=2

Use ...

Date: ...

0·0=0
1·0=0
2·0=0
3·0=0
4·0=0

P-6. Let ... and g(a) ... from the ... & determ...

Sol-n: ...

Inclusion-Exclusion Principle

Calculate total # of students

People who take Algebra

People who take

together: 20+4=24

P.9. use the Euclidean algorithm to find gcd(12, 18)

$0\cdot0=0$	$0\cdot1=0$	$0\cdot2=0$	$0\cdot3=0$	$0\cdot4=0$
$1\cdot0=0$	$1\cdot1=1$	$1\cdot2=2$	$1\cdot3=3$	$1\cdot4=4$
$2\cdot0=0$	$2\cdot1=2$	$2\cdot2=4$	$2\cdot3=1$	$2\cdot4=3$
$3\cdot0=0$	$3\cdot1=3$	$3\cdot2=1$	$3\cdot3=4$	$3\cdot4=2$
$4\cdot0=0$	$4\cdot1=4$	$4\cdot2=3$	$4\cdot3=2$	$4\cdot4=1$

P-6. Deter. whether each of the functions $f(a) = a$ div d and $g(a) = a \bmod d$, where d is a fixed positive integer, from the set of integers to the set of integers is one to one, and determine whether each of these functions is onto.

Soln: If $d=1$, then $f(a)=a$ and $g(a)=0$. Therefore f is clearly one-to-one and onto, and g is neither. If $d>1$, then f is still onto, because $f(db)=b$ for any desired $b\in\mathbb{Z}$, but it is clearly not one to one because $f(0)=f(1)=0$. Furthermore, g is clearly not onto, because its range because $g(0)=g(d)=0$ is just $\{0,1,2,\dots,d-1\}$, and it hits one more number

P-7 Convert the decimal expansion of each of these integers to a binary expansion.

a) 231 b) 4532 c) 97644

Sol: We repeatedly by 2, noting the remainder. The remainders are then arranged in order right obtain the binary representation of the given number.

a) $231:2 = 115$, $r=1$, $a_0=1$ next $115:2 = 57$, $r=1$, $a_1=1$
$57:2 = 28$, $r=1$, $a_2=1$ next $28:2 = 14$, $r=0$, so $a_3=0$
Similarly $a_4=0$ after we divide 14 by 2 obtain 7, $r=0$
3 more divisions yield quotients of 3, 1 and 0, with remainders of 1, 1 and 1 respectively, so $a_5=a_6=a_7=1$. All together
That binary representation is $(a_7,a_6,a_5,a_4,a_3,a_2,a_1,a_0) = (11100111)_2$
As a check we can compute that $2^0+2^1+2^2+2^5+2^6+2^7 = 231$

b) same procedure $4532 = (1000\,1101\,1011\,0100)_2$
Therefore

c) $97644 = (1\,0111\,1101\,0110\,1100)_2$

$r=$

$= b_1 * b_2 * b_3 +$

$m = ((a \bmod m)(b \bmod m)) \bmod m$

$m = ((a \bmod m)(b \bmod m)) \bmod m$

P-8 Convert the binary expan. to a decimal expan.

a) $(1\ 1111)_2$ b) $(10\ 0000\ 0001)_2$ c) $(1\ 0101\ 0101)_2$

d) $(110\ 1001\ 0001\ 0000)_2$.

Sol-n a) $(1\ 1111)_2 = 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 16 + 8 + 4 + 2 + 1 = 31$

An easier way to get the answer is to note that

$(1\ 1111)_2 = (10\ 0000)_2 - 1 = 2^5 - 1 = 31$

b) $(100000\ 0001)_2 = 2^9 + 2^0 = 513$

c) $(1\ 0101\ 0101)_2 = 2^8 + 2^6 + 2^4 + 2^2 + 1 = 256 + 64 + 16 + 4 + 1 = 341$

d) $(1\ 1010\ 0001\ 0000)_2 = 2^{14} + 2^{13} + 2^{11} + 2^8 + 2^4 = 16384 + 8192 + 2048 + 256 + 16 = 26896$

P-9. Find the sum & product of each of these pairs of numbers. Express your answers as a binary expansion.

a) $(100\ 0111)_2$, $(111\ 0111)_2$

b) $(1110\ 1111)_2$, $(1011\ 1101)_2$

c) $(1010\ 1010)_2$, $(1111\ 0000)_2$

d) $(10\ 0000\ 0001)_2$, $(1111\ 1111)_2$

$71 + 119 = 190$

$71 \cdot 119 = 8449$

$239 + 189 = 428$

$239 \cdot 189 = 45,171$

$682 + 496 = 1178$

$682 \cdot 496 = 338,272$

$513 + 1023 = 1536$

$513 \cdot 1023 = 524,799$

P-10. Find the prime factorization of each of the integers.

a) 88

b) 126

c) 729

d) 1001

e) 1111

f) 909,090

Sol-n: In each case we can use trial division, starting with the smallest prime & increasing to the next prime once we find that a given prime no longer is a divisor of what is left. A calculator comes in handy. Alternatively, one could use a factor tree.

a) We note that 2 is a factor of 88 & the quotient upon division by 2 is 44. We divide by 2 again & then again, leaving a quotient of 11. Since 11 is prime, we are done, & we have found the prime factorization

$88 = 2^3 \cdot 11$

This is [illegible]

2. The operations $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b) \bmod m$.
This is multiplication modulo m.
Ex: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Sol'n: Using the definition above:
$7 +_{11} 9 = (7+9) \bmod 11 = 16 \bmod 11 = 5$
$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

Theorem: For $a, b \in Z_m$, $a +_m b \in Z_m$ & $a \cdot_m b \in Z_m$.

Homwork → P-10, (b)
b) $126 = 2 \cdot 63 = 2 \cdot 3 \cdot 21 = 2 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^2 \cdot 7$
c) $729 = 3 \cdot 243 = 3 \cdot 3 \cdot 81 = 3 \cdot 3 \cdot 3 \cdot 27 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 9 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^6$
d) $1001 = 7 \cdot 143 = 7 \cdot 11 \cdot 13$

P-11 How many zeros are there at the end of 100!?
To find the number of zeros at the end of 100! (100 factorial) we need to determine how many times 100! can be divided by 10. Since $10 = 2 \times 5$ & 100! has more factors of 2 than 5, the number of zeros is determined by the number of factors of 5 in 100!
We calculate the number of factors of 5 by dividing 100 by powers of 5 & summing the results:

Number of zeros $= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + \left\lfloor \frac{100}{5^3} \right\rfloor + \dots$

- $\left\lfloor \frac{100}{5} \right\rfloor = 20$
- $\left\lfloor \frac{100}{25} \right\rfloor = 4$
- $\left\lfloor \frac{100}{125} \right\rfloor = 0$ (as $125 > 100$).

Adding these together: $20 + 4 = 24$
Thus, there are 24 zeros at the of 100!

sums.

p12. Use the Euclidean algorithm to find

Date:

a) gcd (12, 18)
b) gcd (111, 201)
c) gcd (1001, 1331)
d) gcd (12345, 54321)
e) gcd (1000, 5040)
f) gcd (9888, 6060)

Sol-n: a) By Lemma 1, gcd (12, 18) is the same as the gcd of the smaller of these 2 numbers (12) & the remainder when the larger (18) is divided by the smaller. In this case remainder is 6; so gcd(12, 18) = gcd(12, 6)
Now gcd (12, 6) is the same as the gcd of the smaller of these 2 numbers (6) & the remainder when the larger (12) is divid. by the smaller, namely 6. This gives gcd (12, 6) = gcd (6, 0) But gcd (x, 0) = x for all positive integers, so gcd (6, 0). Thus the answer is 6. In brief (the form we will use for the remaining parts) gcd (12, 18) = gcd (12, 6) = gcd (6, 0) = 6

b) gcd (111, 201) = gcd (111, 90) = gcd (90, 21) = gcd (21, 6) = gcd (6, 3) = gcd = (3, 0) = 3

c) gcd (1001, 1331) = gcd (1001, 330) = gcd (330, 11) = gcd (11, 0) = 11

d) gcd (12345, 54321) = gcd (12345, 4941) = gcd (4941, 2463) = gcd (2463, 15) = gcd (15, 3) = gcd (3, 0) = 3

e) gcd (1000, 5040) = gcd (1000, 40) = gcd (40, 0) = 40

f) gcd (9888, 6060) = gcd (6060, 3828) = gcd (3828, 2232) = gcd (2232, 1596) = gcd (1596, 636) = gcd (636, 324) = gcd (324, 312) = gcd (312, 12) = gcd (12, 0) = 12

Week 10 Counting (Basics).

Mk-1 1 Addition Rule

2 Multiplic-n Rule