Week 8.

(23)

a) $\gcd(12,18) = \gcd(12,6) = \gcd(6,0) = \underline{6}$

b) $\gcd(111,201) = \gcd(111,90) = \gcd(90,21) = \gcd(21,6) = \gcd(6,3) = \gcd(3,0) = \underline{3}$

c) $\gcd(1001,1331) = \gcd(1001,330) = \gcd(330,11) = \gcd(11,0) = \underline{11}$

d) $\gcd(12345,54321) = \gcd(12345, 4941) = \gcd(4941, 2463) = \gcd(2463,15) = \gcd(15,3) = \gcd(3,0) = \underline{3}$

e) $\gcd(1000,5040) = \gcd(1000,40) = \gcd(40,0) = \underline{40}$

f) $\gcd(9898,6060) = \gcd(6060,3838) = \gcd(3838,2232) = (2232,1596) = (1596,636) = (636,324) = (324,312) = (312,12) = \gcd(12,0) = \underline{12}$

(6) How many zeroes are there at the end of 100! ?

1. How many times 10 is a factor in this factorial. 10 is product of 2 · 5 and 100! has more factors of 2 than 5, num of 0 is determined by num of factors of 5 in 100!

We calc num of factors of 5 by div 100 by powers of 5 and sum the results

Num of zeroes at the end of 100! $= \frac{100}{5} + \frac{100}{5^2} + \frac{100}{5^3} + \dots = 20 + 4 + 0 = \underline{24}$

(3) Find prime factorization of each of these integers:

a) $88 = 2 \cdot 2 \cdot 2 \cdot 11$
$2^3 \cdot 11$ (exponential)

div 88 by the smallest prime num 2 and continue div quotients by 2 till we can't

remaining coefficient 11, i a prime num

b) 63 21 7 1

$126 = 2 \cdot 3 \cdot 3 \cdot 7 = 2^1 \cdot 3^2 \cdot 7^1$ composite nums expressed as a product of prime nums

c) 243 81 27 9 3 1

$729 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = \underline{3^6}$

d) 143 13 1

$1001 = 7 \cdot 11 \cdot 13$

e) $1111 = 11 \times 101$

f) 454545 151515 50505 16835 3367 481 37 1

$909,090 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$

(21) Find sum, product of each of pairs of nums, express answers as binary

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

```
  111
  100  0111
+ 111  0111
-----------
 1110  1110
```

```
   100  0111
 × 111  0111
-----------
   100  0111
  1000  111
 10001  11
000000  0
-----------
1000111
```

$(1110\ 1110)_2$

1000111

1000111

10001110001

b) $(1110 \cdot 1111)_2$ $(10111101)_2$

```
   1110   1111        1+0+1 = 10        1+0 = 1
+  1011   1101        1+1 = 10          0+0 = 0
-------------
   1 1100              1+1+1 = 11
 1101
```

$1110\,1111 \rightarrow 1\cdot2^7+1\cdot2^6+1\cdot2^5+0\cdot2^4+$
$+1\cdot2^3+1\cdot2^2+1\cdot2^1+1\cdot2^0=$
$=128+64+32+8+4+2+1$
$=\underline{239}$

```
x 1110   1111
 00000   000
00000   00

  1110   1111
 11101   111
 ......     .
------------------
1000 1000 1110 0011
```

$1011\,1101 \rightarrow 1\cdot2^7+0\cdot2^6+1\cdot2^5+1\cdot2^4$
$+1\cdot2^3+1\cdot2^2+1\cdot2^1+0\cdot2^0$
$=128+32+16+8+$
$+4+2=189$

428

$1\,1010\,1100 \rightarrow 1\cdot2^8+1\cdot2^7+0\cdot2^6+1\cdot2^5+0\cdot2^4+1\cdot2^3$
$+1\cdot2^2+0\cdot2^1+0\cdot2^0=256+128+$
$+32+8+4=428$

c)
```
+ 110  1010  1010
    1  1111  0000
-----------------
  100  1001  1010
```

```
x 10  1010  1010
   1  1111  0000
------------------------------
      00 00000 00000
     000 00000 000
    0000 00000 00
   00000 00000 0
  1010101010
 1010101010
1010101010
1010101010
------------------------------
1010010100101000000
```

d)

d)
```
  1 1 1 1 1 1 1 1 1
+ 1 0 0 0 0 0 0 0 1
  1 1 1 1 1 1 1 1 1
-----------------------
1 1 0 0 0 0 0 0 0 0 0
```

```
                1 0 0 0 0 0 0 0 1
              × 1 1 1 1 1 1 1 1 1
-----------------------------------
                1 0 0 0 0 0 0 0 1
              1 1 0 0 0 0 0 0 0
            1 0 0 0 0 0 0 0 1
          . . . . . .
-----------------------------------
1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
```

(3) Convert binary expansion into decimal

a) $(1\ 1111)_2 = 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0$

$= 16 + 8 + 4 + 2 + 1 = 31$

b) $(10\ 0000\ 0001)_2 = 1\cdot 2^9 + 0\cdot 2^8 + 0\cdot 2^7 + 0\cdot 2^6 + 0\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = 513$

c) $(1\ 0101\ 0101)_2 = 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = 341$

d) $(110\ 1001\ 0001\ 0000)_2 = 1\cdot 2^{14} + 1\cdot 2^{13} + 0\cdot 2^{12} + 1\cdot 2^{11} + 1\cdot 2^{10} + 1\cdot 2^9 + 1\cdot 2^8 + 0\cdot 2^7 + 0\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0 = 26896$

(4) Convert decimal expansion?

a) $231 = 115$

$231 : 2 = 1$ a_0

$115 : 2 = 1$ a_1

$57 : 2 = 1$ a_2

$28 : 2 = 0$ a_3

$14 : 2 = 0$ a_4

$7 : 2 = 1$ a_5

$3 : 2 = 1$ a_6

$1 : 2 = 1$ a_7

b) $4532 = 1133$

$a_0 = 0$, $a_1 = 0$, $a_2 = 1$, $a_3 = 0$, $a_4 = 1$, $a_5 = 1$, $a_6 = 0$, $a_7 = 1$, $a_8 = 1$, $a_9 = 0$, $a_{10} = 0$, $a_{11} = 0$, $a_{12} = 1$

~~97644~~ $= (1\,0\,0\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0)_2$

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

(47)* $f(a) = a \text{ div } d$

$g(a) = \text{mod } d$ where d is fixed positive int

One to one - function h is one to one if diff inputs produce different outputs if $h(x_1) = h(x_2)$ implies $x_1 = x_2$

Onto (surjective) - every possible output is result of applying function to some input. Formally for every y in codomain there exists x in domain such that $h(x) = y$

if $d = 1$, then $f(a) = a$ and $g(a) = 0$

f is 1 to 1 and onto and g is neither

if $d > 1$, then f is onto, but not 1 to 1 bc $f(0) = f(1) = 0$

g is not onto, range $= \{0, 1, 2, \ldots, d-1\}$ and its not 1 to 1 bc $g(0) = g(d) = 0$.

(48)* write out addition, multiplication tables for $\mathbb{Z}_5$ (where by addition and multiplication we mean $+_5$ and $\cdot_5$)

$0+0=0$ $1+0=1$ $0+2=2$ $0+3=3$

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

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

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

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

$0+4=4$

$1+4=0$

$2+4=1$

$3+4=2$

$4+4=3$

$0\cdot0=0$ $0\cdot1=0$ $0\cdot2=0$ $0\cdot3=0$

$1\cdot0=0$ $1\cdot1=1$ $1\cdot2=1$ $1\cdot3=3$

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

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

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

$0\cdot4=0$

$1\cdot4=4$

$2\cdot4=3$

$3\cdot4=2$

$4\cdot4=1$

---

(4)* if a, b, k and m are ints such that $k \geq 1$, $m \geq 2$, and $a \equiv b$

Theorem 5 implies

$a \cdot a \equiv b \cdot b \pmod{m}$, i.e. $a^2 \equiv b^2 \pmod{m}$

$a \equiv b \pmod m$ and $a^2 \equiv b^2 \pmod m$
we obtain $a^3 \equiv b^3 \pmod m$. after $k-1$
we obtain $a^k \equiv b^k \pmod m$ as desired

(37)* a) let $m = 4$
$c = 2$) nontrivial common factor

Let $a = 0$ and $b = 2$, then $ac = 0$ and $bc = 4$,
so $ac \equiv bc \pmod 4$, but $0 \not\equiv 2 \pmod 4$

b) let $m = 5$, $a = 3$, $b = 3$, $c = 1$ and $d = 6$
then $a^c = 3$ and $b^d = 729 \equiv 4 \pmod 5$,
so $3^1 \not\equiv 3^6 \pmod 5$ even though
$3 \equiv 3 \pmod 5$ and $1 \equiv 6 \pmod 5$.

(19)* $$f(x) = \begin{cases} x \bmod m & \text{if } x \bmod m \le \lfloor m/2 \rfloor \\ (x \bmod m) - m & x \bmod m > \lfloor m/2 \rfloor \end{cases}$$

if m is even, then $f(m/2) = -m/2$

(9) Quotient and remainder? $a = dq + r$

a) $19 : 7$ $\quad$ Dividend = (Divisor × Quotient)
$q = 2 \quad r = 5$ $\quad -111 = 11 \cdot (-11) + 10$

b) $-111 : 11 \quad q = -10 \quad r = 1$?

c) $789 = 2 \quad q = 394 \quad r = 1$

d) $1001 : 13 \quad q = 77 \quad R = 0$

e) $0 : 19 \quad q = 0 \quad R = 0$

f) $3 : 5 \quad q = 0 \quad R = 3 \quad 5 \cdot 0 + 3$

g) $-1 : 3 = 3 \cdot (-1) + 2$, $q = -1$, $r = 2$

h) $4 : 1 = 1 \cdot 4 + 0$ $q = 4$ $r = 0$