HOMEWORK 3 - SOLUTIONS

2. Use $q = \lfloor \frac{13}{3} \rfloor = 4$, then $13 = 4 \cdot 3 + 1$, $0 \leq 1 < 3$.

8. $17 = (-3)(-5) + 2$ $q = -3$, $r = 2$.

16. Answer: 211. $19201 = 5 \cdot 3587 + 1266$, $3587 = 2 \cdot 1266 + 1055$, $1266 = 1 \cdot 1055 + 211$, $1055 = 5 \cdot 211 + 0$ the gcd=211.

18. For 10! and 3^{10} we use the prime factor method. The gcd will contain only the prime 3 because the second number has no other factor than 3.
$10! = (1)(2)(3)(2^2)(5)(2 \cdot 3)(7)(2^3)(3^2)(2 \cdot 5) = (2^7)(3^4)(5^2)(7)$ answer $3^4 = 81$.

22. $a(-5) + b(2) = 1$, $a = 5$, $b = 13$.

27. We shall use the fact that
If d divides a and b and there exist x, y such that $d = ax + by$, then $d = gcd(a, b)$.
$\Rightarrow$
$ax_1 + cy_1 = 1$, $bx_2 + cy_2 = 1$ for some x_1, x_2, y_1, y_2. Then we multiply

$$1 = (ax_1 + cy_1)(bx_2 + cy_2) = ab(x_1x_2) + c(ax_1y_2 + bx_2y_1 + cy_1y_2)$$

and choose $x = x_1x_2$ and $y = ax_1y_2 + bx_2y_1 + cy_1y_2$.
$\Leftarrow$
$abx' + cy' = 1$ then take $x = bx$, $y = y'$ for $gcd(a, c) = 1$ and $x = ax$, $y = y'$ for $gcd(b, c) = 1$.

34. $11x + 15y = 31$ since $gcd(11, 15) = 1$ the equation has infinitely many solutions.
We obtain $11(3) + (-2)(15) = 1$ and thus

$$(x_0, y_0) = 31(3, -2) = (93, 62)$$

(multiply by 31).
The solutions are

$$(93 + 15n, -62 - 11n), \qquad n \in \mathbb{Z}$$

44. Find a non-negative solution of $12x + 57y = 423$. Since $12 = 2^2 \cdot 3$ and $57 = 3 \cdot 19$ then $gcd(12, 57) = 3$. The number $423 = 3 \cdot 141$ which implies that the equation has solutions.
Divide by 3. The equation becomes
$4x + 19y = 141$. Notice that $4(5) + 19(-1) = 1$ we have
$(x_0, y_0) = 141(5, -1) = (705, -141)$ and the general solution
$(x, y) = (705 + 19n, -141 - 4n)$. To determine the positive solutions solve the inequalities:
$705 + 19n \geq 0$ or $n \geq \frac{-705}{19} = -37.1$ finally $n \geq -37$
$-141 - 4n \geq 0$ or $n \leq \frac{-141}{4} = -35.25$ finally $n \leq -36$
we have $n = -36, -37$ the only solutions

$$(21, 3), (2, 7)$$

58. Express 433 in base 5. Answer $433 = (3253)_5$

71.

$$5280 = 528 \cdot 10 = 132 \cdot 4 \cdot 10 = 3 \cdot 11 \cdot 2^5 \cdot 5 = 2^5 3^1 5^1 11^1$$
$$57800 = 289 \cdot 2 \cdot 2^2 \cdot 5^2 = 2^3 5^2 17^2$$

because $289 = 17^2$. Try to divide 289 by 2, 3, ..., 13, 17.

Common prime factors: 2 and 5. The $gcd = 2^3 5^1 = 40$.

76. Only when a, b have opposite signs and $gcd(a, b)|c$. You have to show the details.

82. Let n be the original number. $n = 4n_1 + 1$, where n_1 is how much the first man puts aside for himself. $n - n_1 = 4n_2 + 1$, which also implies that $3n_1 = 4n_2$. Continuing we get $4n_i = 3n_{i-1}$ for $i = 2, 3, 4, 5$. This implies $3^4 n_1 = 4^4 n_5$ and $4^4|n_1$. The minimum number satisfying this condition is $n_1 = 4^4$. This shows that the minimum n is $n = 4 \cdot 4^4 + 1 = 1025$.

92. a) The primes $p \in 2\mathbb{Z}$ are even numbers, since all elements of $2\mathbb{Z}$ are even numbers. We notice that all numbers of the form $p = 2m$, m odd, are prime. If they could be written as $p = p_1 p_2$ with p_1, p_2 prime, then p_1 should contain the factor 2, as well as p_2. In this case, p would be divisible by 4, which is impossible since $2m$ does not contain a factor of 4.

We now show that there are no other prime numbers. Let p prime and let $p = 2^\alpha m$, where m is odd. If $\alpha \geq 2$, then $p = 2^{\alpha-1} \cdot 2m$ and both 2 and $2m$ are prime. It follows that $\alpha \leq 1$. But we know $\alpha \geq 1$ since $p \in 2\mathbb{Z}$. We have shown that $p = 2m$, m odd.

b) Any number $n \in \mathbb{Z}$ can be written as $n = 2^\alpha m$, m odd. Numbers in $2\mathbb{Z}$ have the special property that $\alpha \geq 1$. we have

$$n = 2^{\alpha-1} \cdot 2m\,,$$

where the factors 2 ($\alpha - 1$ times) and $2m$ are prime.

c) The factorization is not unique.

$$72 = 2 \cdot 6^2 = 2 \cdot 2 \cdot 18$$

are distinct factorizations in prime factors.

94. There is a formula for the exponent of p prime in $n!$

$$\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + ...$$

observing that the sum is finite. This gives

$50 + 25 + 12 + 8 + 3 + 1 = 99$ for 2 and

$20 + 4 = 24$ for 5.

The power of 10 is then equal to the smaller one of the two.

Answer 24 zeros.

Proof of the formula for the exponent of a prime in a factorial.

Let a_k be the number of elements among $1, 2, 3 \ldots, n$ which are divisible *exactly* by p^k. It is enough to consider indices k up to $k \leq n$ as the numbers become zero for sure afterwards. The sum

$a_k + a_{k+1} + \ldots a_n = \lfloor \frac{n}{p^k} \rfloor$ equals the number of elements among $1, 2, 3 \ldots, n$ which are divisible by p^k. Notice that we dropped the word *exactly*, since we include factors containing p at higher powers than k.

Exponent of p in $n! = 1 \cdot a_1 + 2 \cdot a_2 + 3 \cdot a_3 + \ldots n \cdot a_n = \sum_{k=1}^{n} \lfloor \frac{n}{p^k}$
which proves the formula.

98. The numbers k between b and a are
$b+1$, $b+2$, ..., $a-1$
$b+1$, $b+2$, ... , $b+(a-b-1)$
Their sum is

$$b(a-b-1) + \frac{1}{2}(a-b-1)(a-b) = \frac{1}{2}(a-b-1)(a+b) = 1000$$

so
$(a-b-1)(a+b) = 2^4 5^3$ Notice that the first facor is necessarily odd, which gives the only possibilities
$a+b = 2^4$, $a-b-1 = 5^3$ impossible because $a+b < a-b-1$
$a+b = 2^4 \cdot 5$, $a-b-1 = 5^2$ i.e. $a = 53$, $b = 27$ (good)
$a+b = 2^4 \cdot 5^2$, $a-b-1 = 5$, i.e. $a = 203$, $b = 197$ (good)
$a+b = 2^4 \cdot 5^3$, $a-b-1 = 1$, i.e. $a = 1001$, $b = 999$ (good)

100. In general, if $d = gcd(a,b)$, $m = lcm(a,b)$ we denote $a' = a/d$, $b' = b/d$. We proved elsewhere that
(i) $gcd(a', b') = 1$
(ii) $m = a'b'd$.

The equality in the problem is $d = gcd(da' + db', da'b')$. We did in class Ex 11 which says that the right hand side is d times $gcd(a' + b', a'b')$. Simplify by d.

We have to show the much simpler identity
$1 = gcd(a' + b', a'b')$ when $gcd(a', b') = 1$.

The simplest proof is to show that $a' + b'$ and $a'b'$ cannot have any common prime factor. We make a proof by contradiction.

Suppose p prime is such that $p|a'+b'$ and $p|a'b'$. Then $p|(a'+b')b'$ and since $p|a'b'$ it must be that $p|(a')^2$. This cannot happen unless $p|a'$ (because p is prime). But $p|a'+b'$ from the assumption, following that $p|(a'+b')-a' = b'$. Since $gcd(a', b') = 1$ we have $p = 1$. So there is no common prime factor between $a' + b'$ and $a'b'$.