ELEMENTARY NUMBER THEORY AND CRYPTOGRAPHY II
SOLUTIONS OF PROBLEM SHEET 1
MICHAELMAS TERM 2014

1. (1) The equality is true for $n = 1$, as both sides are equal to 1.
So suppose the equality is true for some positive n, i.e.

$$P(n): \qquad 1^3 + 2^3 + \cdots + n^3 = \Big(\frac{n(n+1)}{2}\Big)^2 .$$

We need to show that this implies the statement $P(n+1)$ where each n is replaced by $n+1$.
In order to do so, we add $(n+1)^3$ on both sides, which gives

$$1^3 + 2^3 + \cdots + n^3 + (n+1)^3 = \Big(\frac{n(n+1)}{2}\Big)^2 + (n+1)^3 .$$

Now it remains to show that the RHS $\frac{1}{4}\big(n^2(n+1)^2 + 4(n+1)^3\big)$ equals the right hand side of $P(n)$ with n replaced by $n+1$, i.e. to $\Big(\frac{(n+1)^2(n+2)^2}{2}\Big)^2$. Indeed, both terms equal $\frac{1}{4}\big((n+1)^2(n^2+4(n+1))$, and we are done.

(2) This time the case $n = 1$ gives $1 - 8 + 27$ for the LHS, which is equal to 20, while the RHS gives $2^2 \cdot 5$ which is indeed the same.
So suppose the equality is true for some positive n, i.e.

$$P(n): \qquad 1^3 - 2^3 + 3^3 - + \cdots - (2n)^3 + (2n+1)^3 = (n+1)^2(4n+1) .$$

We need to show that this implies the statement $P(n+1)$.
Again, we check that the difference of the LHSs of $P(n+1)$ and $P(n)$, i.e. $(2n+3)^3 - (2n+2)^3$, is the same as the difference of the RHSs, i.e. $(n+2)^2(4n+5) - (n+1)^2(4n+1)$.
By expanding into powers of n, we find $3(12n^2 + 54n) + 3^3 - 3(8n^2 + 24n) - 2^3$ on the LHS, which amounts to $12n^2 + 30n + 19$; on the RHS we get $4n(n^2 + 4n + 4 - n^2 - 2n - 1) + 5n^2 + 20n + 20 - n^2 - 2n - 1)$, i.e. $4n(2n+3) + 4n^2 + 18n + 19$ which is easily seen to be the same expression.

Taking the difference of the second equation for $P(n)$ and $P(n-1)$ we find on the left n^3, while on the right we get $\Big(\frac{n(n+1)}{2}\Big)^2 - \Big(\frac{n(n-1)}{2}\Big)^2$, a difference of two squares.

2. (a) For $n = 1$ we have $13 \mid 4^3 + 3^3 = 64 + 27 = 91$, which is indeed true.
Suppose now we know that 13 divides $4^{2n+1} + 3^{n+2}$ for some n. Then we need to deduce from this that 13 divides $4^{2n+3} + 3^{n+3}$.
Similar to the example done in the lectures we use the fact that $a|b$ and $a|c$ inplies that $a|b + c$. In paerticular it suffices to show that

13 divides the difference b between two successive members, i.e. $b = 4^{2n+3} + 3^{n+3} - (4^{2n+1} + 3^{n+2})$. But

$$\begin{aligned} b &= 4^{2n+3} - 4^{2n+1} + 3^{n+3} - 3^{n+2} \\ &= 4^{2n+1}(4^2 - 1) + 3^{n+2}(3 - 1) \\ &= 4^{2n+1}(13 + 2) + 3^{n+2} \cdot 2 \\ &= 4^{2n+1} \cdot 13 + 2(4^{2n+1} + 3^{n+2}) \end{aligned}$$

and the latter expression is clearly divisible by 13 (the second term by induction assumption).

Note that, with hindsight, a quicker proof results from using the smaller member with a different multiple (here 3), i.e. using $b' = 4^{2n+3} + 3^{n+3} - 3(4^{2n+1} + 3^{n+2})$, as this would have canceled two of the four terms, leaving $b' = 4^{2n+1}(4^2 - 3)$, the second factor of which being obviously divisible by 13.

(b) For $n = 1$ we have $3^{3n+1} + 2^{n+1} = 3^4 + 2^2 = 85$ which is equal to $17 \cdot 5$, hence indeed divisible by 5.

Suppose now we know that 5 divides $3^{3n+1} + 2^{n+1}$ for some n. Then we need to deduce from this that 5 divides $3^{3n+4} + 2^{n+2}$.

Again we consider the difference of two successive expressions, i.e. $3^{3n+4} + 2^{n+2} - (3^{3n+1} + 2^{n+1})$; regrouping them, we write this as $3^{3n+1}(3^3 - 1) + 2^(n + 1)$, and then write the factor $3^3 - 1$ as $5^2 + 1$, hence $3^{3n+1}(3^3 - 1) + 2^(n + 1) = 3^{3n+1} \cdot 5^2 + 3^{3n+1} + 2^{n+1}$, of which the first term clearly is divisible by 5 while the remaining sum is divisible by 5 by our induction assumption. This proves the claim.

3. (a) If $c \mid a$ and $\mid b$ then $a = ca_1$ and $b = cb_1$s for some integer a_1, b_1. Then $ma + nb = cma_1 + cnb_1 = c(ma_1 + nb_1)$ which proves the problem.

(b) We first discuss the case when at least one of a and b is zero: this can only happen if both a and b are zero ⟦since 0 does not divide any non-zero number⟧, and in this case the claim is clear.

Now let a, b be non-zero. If $a \mid b$ and $b \mid a$, then $a = mb$ for some $b \in \mathbb{Z}$ and $b = na$ for some $n \in \mathbb{Z}$. Hence $a = m(na) = (mn)a$ ⟦by associativity of multiplication⟧and hence $mn = 1$. In particular m and n divide 1, and the only divisors of 1 are 1 and -1.

4. (a) Simple solution: since all numbers involved are positive, we can simply cancel a in the equation $ac = abn$ for some $n \in \mathbb{Z}$.

(b) This is not a valid statement: choose, for some $a > 1$, $b = a^3$ and $c = a^2$.

Then $b^2 = a^6 = c^3$ and in particular $b^2 \mid c^3$. But $b = a^3 \nmid a^2 = c$ (since clearly $a^3 > a^2$ and since divisors are not greater than the number which they divide).

(Note: Providing just an example $b = 8, a = 4$ will be enough for the solution.)

(c) First Proof. We start by proving the result for coprime a and b. If $\gcd(a, b) = 1$ then one can represent $1 = ax + by$ for $x, y \in \mathbb{Z}$. Squaring this equality gives

$$1 = (ax)^2 + 2abxy + (by)^2 = a \cdot (ax^2 + 2bxy) + b^2\dot{y}^2.$$

Therefore $\gcd(a, b^2) = 1$. By repeating the same argument we get $\gcd(a^2, b^2) = 1$.
Now put $d = \gcd(a, b)$; we are allowed to use 6a) which says here that, since $d \mid a$ and $d \mid b$, the integers a/d and b/d satisfy $\gcd(a/d, b/d) = 1$. From here we deduce $\gcd((a/d)^2, (b/d)^2) = 1$, and applying Q.6a) again, we find $\gcd(a^2, b^2) = d^2$.
Second proof (using FTA): if we factor $a = \prod_p p^{\alpha(p)}$ and $b = \prod_p p^{\beta(p)}$, where the product runs over all primes p, and all but finitely many exponents $\alpha(p)$, $\beta(p)$ are zero, then note that $\gcd(a, b) = \prod_p p^{\min(\alpha(p),\beta(p))}$. Therefore

$$\gcd(a, b)^2 = \prod_p p^{2\min(\alpha(p),\beta(p))},$$

while

$$\gcd(a^2, b^2) = \prod_p p^{\min(2\alpha(p),2\beta(p))}.$$

But the latter two products agree since $r\min(s, t) = \min(rs, rt)$ for any positive r, s, t.

(d) It is not true. For example, $3 \nmid 4, 4 \nmid 6$ but $3|6$.

5. (a) We use multiple times the fact that $\gcd(a, b) = \gcd(a, b - qa)$ for $a, b, q \in \mathbb{Z}$ (as a substitute for the not yet available Euclidean algorithm).
Successive subtraction and possible swapping of roles gives

$$\begin{aligned}\gcd(455, 1235) &= \gcd(455, 1235 - 2 \cdot 455) = \gcd(455, 325)\\ &= \gcd(325, 455) = \gcd(325, 455 - 325) = \gcd(325, 130)\\ &= \gcd(130, 325) = \gcd(130, 325 - 2 \cdot 130) = \gcd(130, 65)\\ &= \gcd(65, 130 - 2 \cdot 65) = \gcd(65, 0) = 65.\end{aligned}$$

If we backtrace which multiples we have used then we can find integers x and y such that $65 = 455x + 1235y$, as in the Euclidean algorithm: we have used $65 = 325 - 2 \cdot 130$, $130 = 455 - 325$ and $325 = 1235 - 2 \cdot 455$. Successively substituting all these gives

$$65 = 325 - 2 \cdot (455 - 325) = 3 \cdot 325 - 2 \cdot 455 = 3 \cdot (1235 - 2 \cdot 455) - 2 \cdot 455$$

i.e., $65 = 3 \cdot 1235 - 8 \cdot 455$, and so $x = -8$, $y = 3$ do it.

(b) Exactly like (a), $d = 211$ and $(x, y) = (4, -3)$ suffice.

6. a) Put $g = \gcd(an, bn)$ and $d = \gcd(a, b)$, then on one hand we have, for some $x, y \in \mathbb{Z}$, that $g = anx + bny = n(ax + by)$, but also $d \mid ax + by$, so $dn \mid g$, and in particular $dn \leq g$.
On the other hand, writing $d = ax' + by'$ implies that $dn = anx' + bny'$. Now $g|an, g|dn$ and therefore $g|dn \Rightarrow g \leq dn$. So finally we get $g = dn$.

Yet another proof, by induction on $a + b$: the statement is clear for $a = b = 1$, since $\gcd(n, n) = n \cdot 1$.
Now suppose the statement is true for $a, b \geq 1$ such that $a + b < k$ for some integer k. Then we want to show it for k.

We can assume, up to swapping roles for a and b, that $a \leq b$. Then, putting $b' = b - a$ for which we have $0 \leq b' < b$, we get

$$\gcd(an, bn) = \gcd(an, bn - an) = \gcd(an, b'n) = n \gcd(a, b')\,,$$

the latter equality by induction assumption. But then $\gcd(a, b') = \gcd(a, b)$, and we are done.

b) Now suppose a, b and m are positive integers with $m \mid a$ and $m \mid b$, i.e. we write $a = mr$ and $b = ms$ for some integers r, s. Then we need to show that $m \mid \gcd(a, b)$: for some integers x, y, we have

$$\gcd(a, b) = ax + yb = (mr)x + (ms)b = m(rx + sb)\,,$$

hence m indeed divides $\gcd(a, b)$.

7. This question is somewhat of a challenge: following the hint, and simply using $x^2 - 1 = (x + 1)(x - 1)$ one gets

$$F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = F_{n-1}(F_{n-1} - 2)\,,$$

and by induction one finds $F_n - 2 = \prod_{j=0}^{n-1} F_j$ (note that $F_0 = 3$ and hence the process stops with $F_0 - 2 = 1$).

Hence $\gcd(F_j, F_n) \mid 2$ for any $j = 0, \ldots, n - 1$. But since all the F_j are odd (we add 1 to a non-trivial power of 2), that gcd must be 1.

8. Let's prove this by induction on n: it is obvious for $n = 1$ (i.e. $\gcd(F_0, F_1) = 1$). Suppose it is true for all $k < n$. Then we want to show it for n, i.e. $\gcd(F_{n-1}, F_n) = 1$.

But using a lemma from the lectures we get

$$\gcd(F_n, F_{n+1}) = \gcd(F_n, F_{n+1} - F_n)\,,$$

and the latter is simply equal to $\gcd(F_n, F_{n-1})$, which by induction assumption is 1.

9. (a) We can use the polynomial identity

$$x^n - 1 = (x^{n-1} + x^{n-2} + \cdots + x + 1)(x - 1)\,,$$

and plug in $x = a$ for $a \in \mathbb{Z}$.

(b) Using that, for $a \neq 1$ and any $n \geq 1$, we have (from (a))

$$\frac{a^n - 1}{a - 1} = a^{n-1} + a^{n-2} + \cdots + a + 1\,,$$

we can write the right hand side as

$$(a^{n-1} - 1) + 1 + (a^{n-2} - 1) + 1 + \cdots + (a - 1) + 1 + 1\,,$$

and we find n terms 1 outside the parentheses. By (a), we know that $a-1$ divides each term in parentheses, and we can use our Proposition stating that $\gcd(c, b) = \gcd(c, b - c) = \cdots = \gcd(c, b - qc)$ for any $b, c, q \in \mathbb{Z}$ to get

$$\gcd\left(\frac{a^n - 1}{a - 1}, a-1\right) = \gcd\left((a^{n-1}-1)+(a^{n-2}-1)+\cdots+(a-1)+n, a-1\right) = \gcd(n, a-1)$$

(use that proposition with $c = a-1$, $b = \frac{a^n-1}{a-1}$ and $q = \sum_{j=1}^{n-1} \sum_{k=0}^{j-1} a^k$).

10. (a) Note that there can not be two consecutive odd numbers. Therefore one of the consecutive numbers is divisible by 2 and so is their product.

(b) Note that each odd number is of the form $b = 2k + 1$ for some $k \in \mathbb{Z}$. Then $b^2 - 1 = (2k + 1)^2 - 1 = 4k(k + 1)$. From the part (a) of the problem we know that $2|k(k + 1)$ so finally $8|4k(k + 1)$.