Theory of Numbers homework 1
Divisibility
Due September 17th, 2018

Exercise 1. Let $a, b, c \in \mathbb{Z}$. Show that if $a|b$ and $a|c$, then for all integers $k, l$, we have $a|kb + lc$.
Solution. $a|b$ implies that there exists $s \in \mathbb{Z}$ such that $sa = b$. Analogously, $a|c$ implies that there exists $t \in \mathbb{Z}$ such that $ta = c$. Multiplying these equations by $k$ and $l$ respectively, we find that $ksa = kb$ and $lta = lc$. Then, $ksa + lta = kb + lc$. Factoring out $a$ from the left hand side, we have that $(ks + lt)a = kb + lc$. In particular, we have that $a|(kb + lc)$.

Exercise 2. 1. Show that any integer can be written in exactly one of the forms $4k$, $4k + 1$, $4k + 2$ or $4k + 3$ for some integer $k$.
Solution. Let $a$ be an integer. Writing its Euclidean division by 4, we get that $a = 4q + r$ where $q$ and $r$ are unique integers such that $0 \leq r < 4$. This means that $r$ can be equal to 0, 1, 2 or 3, so $a$ is equal to $4q$, $4q + 1$, $4q + 2$ or $4q + 3$. Moreover, by uniqueness of $q$ and $r$, $a$ cannot be written in two of these forms.

2. Show that the square of an even integer is of the form $4k$ for some integer $k$, and that the square of an odd integer is of the form $4k + 1$ for some integer $k$.
Solution. Let $x \in \mathbb{Z}$ be an even integer. Then for some $n \in \mathbb{Z}$ we can write $x = 2n$. Then $x^2 = (2n)^2 = 4n^2$. Taking $n^2 = k$, we have that $x^2 = 4k$.

Let $x \in \mathbb{Z}$ be an odd integer. Then for some $n \in \mathbb{Z}$ we can write $x = 2n + 1$. Then
$$x^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 4(n^2 + n) + 1$$
whence it follows that $x^2 = 4k + 1$ if we set $k = n^2 + n$.

Exercise 3. Show that for all integers $a, b$ with $b > 0$, there exist unique integers $q$ and $r$ such that $a = bq + r$ and $b \leq r < 2b$.
Solution. If we have $a = bq + r$ with $b \leq r < 2b$, then we have
$$a = b(q + 1) + (r - b),$$
where $0 \leq r - b < b$. Thus, $q' = q + 1$ and $r' = r - b$ are exactly the quotient and remainder in the Euclidean division of $a$ by $b$. By uniqueness of $q'$ and $r'$, the integers $q$ and $r$, given by $q = q' - 1$ and $r = r' + b$ satisfy the above conditions, and are unique.

Exercise 4. Show that if $(x, y, z)$ is a Pythagorean triple, that is, an integral solution of the equation
$$x^2 + y^2 = z^2,$$
thn exactly one of the following holds:
1. $x, y, z$ are all even;
2. $x$ and $z$ are odd and $y$ is even;
3. $y$ and $z$ are odd and $x$ is even.
Solution. First of all, note that for an integer \( x \), \( x^2 \) is even (resp. odd) if and only if \( x \) is even (resp. odd). (This follows from Exercise 2: there, we showed that a square of an even number is of the form \( 4k \), so it is even, and the square of an odd integer is of the form \( 4k + 1 \), so it is odd. Conversely, if for some integer \( x \), \( x^2 \) is even, then it is not of the form \( 4k + 1 \), so by the result of Exercise 2, \( x \) cannot be odd and must therefore be even. The same argument proves that if \( x^2 \) is odd, then \( x \) is odd. )

Next, notice that conditions 1, 2, 3 are mutually exclusive, so that it will be sufficient to show that they are the only possibilities.

Suppose \( x \) is even. If \( y \) is also even, then \( 2 | (x^2 + y^2) \) so that \( 2 | z^2 \). So, \( 2 | z \). That is, condition 1 holds. Suppose that \( x \) is even while \( y \) is odd. Then \( 2 | x^2 \) and \( 2 \nmid y^2 \). So, \( 2 \nmid z^2 \). Thus, \( z \) is odd. This is condition 3.

Suppose that \( x \) is odd. If \( y \) is even, then \( x^2 + y^2 \) is odd. So, \( z^2 \) is odd, and we see that \( z \) is odd. This is condition 2. If \( x \) is odd and \( y \) is odd, then \( x^2 + y^2 = z^2 \) is even and \( z \) must be even. So, \( z = 2n \), and we write \( z^2 = 4n^2 \). Then \( 4 | z^2 \). This implies that \( 4 | (x^2 + y^2) \). But, \( x^2 = 4k + 1 \) and \( y^2 = 4j + 1 \), by Exercise 2. So, \( x^2 + y^2 = 4(k + j) + 2 \). Thus, \( 4 \nmid (x^2 + y^2) \), which is a contradiction. So, this equation has no solutions when both \( x \) and \( y \) are odd.

In conclusion, the only possibilities are conditions 1, 2, and 3. By mutual exclusivity, exactly one of them holds for any triple \( (x, y, z) \in \mathbb{Z}^3 \) satisfying \( x^2 + y^2 = z^2 \).

Exercise 5. 1. Compute \( \gcd(201, 694) \).

Solution. We apply the Euclidean algorithm:

\[
\begin{align*}
694 &= 201 \times 3 + 91 \\
201 &= 91 \times 2 + 19 \\
91 &= 19 \times 4 + 15 \\
19 &= 15 \times 1 + 4 \\
15 &= 4 \times 3 + 3 \\
4 &= 3 \times 1 + 1
\end{align*}
\]

Therefore \( \gcd(694, 201) = 1 \).

2. Find integers \( u \) and \( v \) such that \( 694u + 201v = \gcd(201, 694) \).
Solution. We apply the reversed Euclidean algorithm:

\[
1 = 4 - 3 \times 1 \\
= 4 - (15 - 4 \times 3) \times 1 \\
= 4 \times 4 - 15 \times 1 \\
= (19 - 15 \times 1) \times 4 - 15 \times 1 \\
= 19 \times 4 - 15 \times 5 \\
= 19 \times 4 - (91 - 19 \times 4) \times 5 \\
= 19 \times 24 - 91 \times 5 \\
= (201 - 91 \times 2) \times 24 - 91 \times 5 \\
= 201 \times 24 - 91 \times 53 \\
= 201 \times 24 - (694 - 201 \times 3) \times 53 \\
= 201 \times 183 - 694 \times 53.
\]

Therefore, \( u = 183 \) and \( v = -53 \) work.

Exercise 6. 1. (a) Show that for any \( a, n \in \mathbb{Z} \), \( \gcd(a, a + n) \) divides \( n \).

Solution. Set \( d = \gcd(a, a + n) \). Then, \( d \mid a \) and \( d \mid (a + n) \). It follows that \( d \mid (a + n - a) \). That is, \( d \mid n \).

(b) Deduce from this that \( a \) and \( a + 1 \) are always relatively prime.

Solution. Let \( d = \gcd(a, a + 1) \). Then \( d \mid 1 \) by (a). Since \( d \) is positive, this implies \( d = 1 \). Hence, \( \gcd(a, a + 1) = 1 \).

(c) Give an example where \( \gcd(a, a + n) \) is not equal to \( n \).

Solution. Take \( a = 2, n = 4 \), so \( a + n = 6 \). Thus, \( \gcd(2, 6) = 2 \neq 4 \).

2. Let \( a \) and \( b \) be two integers such that \( \gcd(a, b) = 1 \). Show that \( \gcd(a + b, a - b) \) is equal either to 1 or to 2.

Solution. Set \( d = \gcd(a - b, a + b) \). Then \( d \mid (a + b) \) and \( d \mid (a - b) \), so \( d \) divides \( (a + b) + (a - b) = 2a \) on the one hand, and \( (a + b) - (a - b) = 2b \) on the other hand. Therefore, \( d \mid \gcd(2a, 2b) \) by remark 2.3.6 in the lecture notes. But \( \gcd(2a, 2b) = 2 \gcd(a, b) = 2 \), so \( d \mid 2 \). Since \( d \) is positive, \( d = 1 \) or \( d = 2 \).

3. Let \( a, b, c \) be integers such that \( \gcd(a, b) = 1 \) and \( \gcd(a, c) = 1 \). Show that \( \gcd(a, bc) = 1 \).

Solution. Because \( \gcd(a, b) = 1 \), we can find coefficients \( s, t \in \mathbb{Z} \) such that

\[
sa + tb = 1.
\]

Multiply both sides of the equation by \( c \) to get

\[
csa + tbc = c.
\]

Now, let \( d \) be such that \( d \mid a \) and \( d \mid bc \). Then by the preceding equation, we have that \( d \mid c \). Then, \( d \mid a \) and \( d \mid c \), so \( d \leq \gcd(a, c) = 1 \). Hence, \( d = 1 \). Therefore, \( \gcd(a, bc) = 1 \).