HOMEWORK 1: OUR FIRST EXAMPLE

MIKE SORICE

Questions

Exercise 1. A natural number, $m \in \mathbb{N}$, is *divisible* by $a \in \mathbb{N}$ if there is a number $d \in \mathbb{N}$ so that $da = m$. Consider the following statement:

If m is divisible by six, then it is divisible by three.

(1) Give a direct proof of this statement.

Proof. Given $6|m$, by definition, $\exists d \in \mathbb{N}$ s.t. $m = 6d = 3(2d)$.
$\therefore \exists d' \in \mathbb{N}$ s.t. $m = 3d'$, namely $d' = 2d$. □

(2) Give the contrapositive of the statement.
If m is not divisible by 3, then it is not divisible by 6.

(3) Give a proof by contrapositive of the statement.

Proof. Suppose $3 \not| m$.
Then by definition, $\nexists d \in \mathbb{N}$ s.t. $m = 3d$, i.e. $\forall d \in N, m \neq 3d$.
A fortiori, there is no even natural number $2d'$ such that $m = 3(2d') = 6d'$ for $d' \in \mathbb{N}$.
$\therefore 6 \not| m$. □

(4) Give a proof by contradiction of the statement.

Proof. Given $6|m$, suppose for contradiction $3 \not| m$.
$6|m \Rightarrow \exists d \in \mathbb{N}$ s.t. $m = 6d = 3(2d)$, but $d \in \mathbb{N} \Rightarrow 2d \in N$.
$\therefore \exists 2d = d' \in \mathbb{N}$ s.t. $m = 3d'$.
$\therefore 3|m$ by definition. $\Rightarrow\!\Leftarrow$ □

Exercise 2 (Hungerford, 1.1.8)**.** Use the Division Algorithm to show that every odd integer is either of the form $4k + 1$ or of the form $4k + 3$ for some integer k.

Proof. Let z be some odd integer.
By the division algorithm, $\exists!(q, r) \in \mathbb{Z}^2$ with $0 \leq r < 2$ s.t. $z = 2q + r$.
Since z is odd, by definition, $2 \not| z \Rightarrow r \neq 0 \Rightarrow r = 1$ so that $z = 2q + 1$.
q being an integer, $\exists!(k, l) \in \mathbb{Z}^2$ with $0 \leq l < 2$ s.t. $q = 2k + l$ by the division algorithm.
l is either 0 (if q is even) or 1 (if q is odd.)

$$\therefore z = 2(2k+l)+1 = 4k+2l+1 = \begin{cases} 4k+1, & l=0 \\ 4k+3, & l=1 \end{cases}$$

□

Exercise 3. Suppose that $a|c$ and $b|c$. Show that it is *not necessarily true* that $ab|c$, but that it *is* true if $(a,b)=1$.

It is not the case that $a|c \wedge b|c \Rightarrow ab|c$.

Proof. Let $a=b=c=2$. $2|2$ and $2|2$, yet $2 \cdot 2 = 4 \not| 2$. □

However, is is the case that $a|c \wedge b|c \wedge (a,b)=1 \Rightarrow ab|c$.

Proof. Suppose $a|c \wedge b|c \wedge (a,b)=1$.

$a|c \Rightarrow c = ma$ for some $m \in \mathbb{Z}$ so that $b|c \Rightarrow b|ma$.

As $b|ma \wedge (a,b)=1$, $b|m$ by theorem 1.4 so that $\exists n \in Z$ s.t. $m = bn$.

$\therefore c = nab \Rightarrow ab|c$ by definition. □

Exercise 4 (Hungerford, 1.3.21)**.** Suppose that $c^2 = ab$ and $(a,b)=1$. Use the Fundamental Theorem of Arithmetic to show that a and b must be squares. Then explain why the assumption $(a,b)=1$ is necessary.

Proof. We require $a,b>0$ as otherwise the statement to prove holds for, for example, $a=-1, b=-4, c=2$ (as $-1 \cdot -4 = 4 = 2^2 \wedge (-1,-4)=1$,) though -1 and -4 are not squares.

Consider the case $c=0$. Then $ab=c^2=0$ entails that at least one of a or b is 0, so that $(a,b)=1$ and $a,b>0$ require that the other is 1. $0=0^2$ and $1=1^2$ are squares.

Consider $c \neq 0 \Rightarrow c^2 > 0$. If one of a,b is $1=1^2$, then the other is necessarily c^2, a square.

It remains to consider the case $c \neq 0 \wedge a,b>1$. Given $a,b>1$, by the F.T.A., there are unique positive primes $P=\{p_i\}_{i=1}^{l}$ and $Q=\{q_i\}_{i=1}^{m}$ such that $a=\prod P$ and $b=\prod Q$.

Further, by the F.T.A., there are unique (up to sign) primes $R=\{r_i\}_{i=1}^{n}$ such that $c=\prod R \Rightarrow c^2 = \prod_{i=1}^{n} r_i^2$.

$\forall p \in P, p|a$ as $a=\prod P$, so $p|ab \Rightarrow p|c \Rightarrow p|\prod R$.

$\therefore$ as p is prime by hypothesis, $\forall p \in P, p|r$ for some $r \in R$ by corollary 1.6.

r being prime and $p>1$ by hypothesis, $p|r \Rightarrow p=r$ by corollary 1.6. $\therefore \forall p \in P, \exists r \in R$ s.t. $p=r$.

Similarly, $\forall q \in Q, \exists r \in R$ s.t. $q=r$.

Now, $\forall p \in P, p \notin Q$ as otherwise a and b would share at least $p > 1$ as a divisor, but $(a,b) = 1$. Similarly, $\forall q \in Q, q \notin P$ so that $P \cap Q = \emptyset$.

Thus, as $\prod\limits_{i=1} nr_i^2 = \prod P \prod Q$, $\forall r \in R, r^2 | \prod P \prod Q \Rightarrow r | \prod P \prod Q$.

As $\prod P \prod Q$ is a product of primes and r is prime by hypothesis, $\exists s \in P \cup Q$ s.t. $r|s$ by corollary 1.6. Further, s and r being prime, $s = \pm r$.

$P \cap Q = \emptyset$, so each $r \in R$, $|r|$ appears in exactly one of P or Q.

Suppose $|r| \in P$. Then a can be divided by $|r|$ twice as $ab = c^2$ and $r^2 | c^2$. Therefore P contains $|r|$ twice for each $r \in R$. Without loss of generality, let $|r_i| \in P$ for $i \in \left\{1, ..., \frac{l}{2}\right\}$ (so that $|r_i| \in Q$ for $i \in \left\{\frac{l}{2}+1, ..., n\right\}$) and $|r_i| \leq |r_{i+1}|$ for $i \in \{1, ..., n-1\}$. Then $a = \prod\limits_{i=1}^{l} p_i = \prod\limits_{i=1}^{l/2} r_i^2 = \left(\prod\limits_{i=1}^{l/2} |r_i|\right)^2$, which is a square.

Similarly, for $|r_i| \in Q$ for $i \in \left\{\frac{l}{2}+1, ..., n\right\}$, $b = \left(\prod\limits_{i=l/2+1}^{n} |r_i|\right)^2$, which is also a square.

□

As suggested in the above proof, the result requires that $(a,b) = 1$ as otherwise a factor of c might divide both a and b, so that they could multiply to a square (i.e. a product of squares) without being squares themselves. Consider, for example, $2 \cdot 2 = 4 = 2^2$. Neither a nor b is a square, yet since they share a common factor (2,) they can multiply to produce a square (4.)

Exercise 5 (Hungerford, 1.3.26)**.** Show that, for any $n \in \mathbb{N}$, there exists a list of n consecutive composite integers. Try starting your list with

$$(n+1)! + 2.$$

Proof. For $n = 0$, the claim is vacuously true.

For $n = 1$, the single integer $(1+1)! + 2 = 4$, being composite ($4 = 2^2$) will do.

Suppose $n > 1$ then. Consider $(n+1)! + m = \prod\limits_{i=1}^{n+1} i + m$ for $m \in \mathbb{N} \wedge 2 \leq m \leq n+1$:

$$(n+1)! + m = \prod_{i=1}^{n+1} i + m = m\left(1 + \frac{1}{m}\prod_{i=2}^{n+1} i\right) = m\left(1 + \prod_{i \in \{1,2,...,n+1\} - \{m\}} i\right).$$

Now, $\prod\limits_{i \in \{1,2,...,n+1\} - \{m\}} i = \frac{(n+1)!}{m}$, being a product of integers, is an integer so that $m | [(n+1)! + m]$ so that $(n+1)! + m$ is composite by definition.

As the above holds for $m \in \mathbb{N}, 2 \leq m \leq n+1$, it produces a set of n consecutive positive integers, $\{(n+1)!+2, (n+1)!+3, ..., (n+1)!+n+1\}$ all of which are composite as $2|\left[(n+1)!+2\right], 3|\left[(n+1)!+3\right]$, *etc.*

□

Exercise 6. Suppose c and b are natural numbers and $c > b > 0$. Show that there exists a natural number r so that $b|(c-r)$ and that if we require $0 \leq r < b$, then this r is unique.

Proof. $b, c \in \mathbb{N} \Rightarrow b, c \in \mathbb{Z}$ as $\mathbb{N} \subset \mathbb{Z}$.

$\therefore \exists!(q,r) \in \mathbb{Z}^2$ s.t. $c = bq + r \wedge 0 \leq r < b$ by the division algorithm.

$r \in \mathbb{Z} \wedge 0 \leq r \Rightarrow r \in \mathbb{N}$.

$\therefore c - r = bq \Rightarrow b|(c-r)$.

$c - r > 0$ as $r < b < c$ by hypothesis, and $c - r = bq \Rightarrow bq > 0$. $b > 0$ as well by hypothesis, so $q > 0$. $q \in \mathbb{Z} \wedge q > 0 \Rightarrow q \in \mathbb{N}$.

□