Problem 1. Let us say that a natural number $p$ has Euclid's Property (EP) if the following is true:

(EP) Whenever $a, b$ are integers such that $p$ divides the product $ab$, it follows that $p$ divides $a$ or $p$ divides $b$.

That is, $p$ has the EP if

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(p \mid ab \implies (p \mid a \lor p \mid b)).$$

Euclid’s Lemma says that every prime number has the EP. **Prove** that if a natural number $p$ has the EP, and $p > 1$, then $p$ is a prime number.

Problem 2. For each of the four pairs $(a, b)$ of integers listed below,

(a) **find** the greatest common divisor $d$ of $a$ and $b$,

(b) **find** integers $m, n$ such that $d = ma + nb$.

i. $a = 22, b = 28$,  
ii. $a = 23, b = 28$,  
iii. $a = 23, b = 41$,  
iv. $a = 101, b = 69$.

(Here is an example: if $a = 8$ and $b = 5$, then $d = 1$, and we can take $m = -8, n = 13$. This works, because $(-8) \times 8 + 13 \times 5 = -64 + 65 = 1$, so $d = ua + vb$.)

---

1. When you solve a problem that has a specific, short answer (such as, for example, “find $d$ such that ... and then find integers $m, n$ such that ...”) you should always indicate very clearly which of the many numbers and other things that you have written is supposed to be your answer, as I have done in the example by putting them in boxes. **Never write a dozen different numbers or formulas, one of which happens to be your answer, without telling me which one is your answer.**
**Problem 3.** Bézout’s lemma says that, if \( a, b \) are integers, \( a \neq 0 \) or \( b \neq 0 \), and \( d \) is the greatest common divisor of \( a \) and \( b \), then there exist integers \( u, v \) such that \( d = ua + vb \). Here you are asked to prove a stronger result, in the case when both \( a \) and \( b \) are nonzero.

**Prove** that

(*) if \( a, b \) are integers such that both \( a \) and \( b \) are different from 0, and \( d \) is the greatest common divisor of \( a \) and \( b \), then

(*.1) there exist integers \( u, v \) such that

(*.1.a) \( d = ua + vb \),
(*.1.b) \( u \geq 0 \),
and
(*.1.c) \( u < |b| \) and \( |v| \leq |a| \),

and

(*.2) there exist integers \( u', v' \) such that

(*.2.a) \( d = u'a + v'b \),
(*.2.b) \( v' \geq 0 \),
and
(*.2.c) \( |u'| \leq |b| \) and \( v' < |a| \),

(Here is an example: if \( a = 8 \) and \( b = 5 \), then \( d = 1 \), and you can take \( u = 2 \), \( v = -3 \), \( w = -3 \), \( x = 5 \). Then conditions (*.1.a), (*.1.b), (*.1.c), (*.2.a), (*.2.b), (*.2.c) are satisfied.)

**HINT:** Using Bezout’s lemma, start with some way of expressing \( d \) as \( ma + nb \) with \( m, n \) integers. Then use the division theorem to write \( m = bq + r \), with \( q, r \in \mathbb{Z} \) and \( 0 \leq r < |b| \). Then show that, for an integer \( s \) (for which you will have an explicit formula), \( d = ra + sb \). Then prove that \( |s| \) must be less than or equal to \( |a| \). (For this, you will use the basic properties of the absolute value, in particular the triangle inequality, and the property that \((\forall x \in \mathbb{R})(\forall y \in \mathbb{R})|xy| = |x| \cdot |y| \). And you should also use the fact that \( d \leq |a| \).) So, taking \( u \) to be \( r \), and \( v \) to be \( s \), you get (*.1). The argument for (*.2) is similar.
Problem 4. For each of the four pairs $a, b$ of Problem 2, find integers $u, v, u', v'$ that satisfy the conditions of Problem 3.

Problem 5. If $n$ is a positive integer, we use $\mathbb{Z}_n$ to denote the set of all integers $x$ such that $0 \leq x < n$. (For example, $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$, $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.)

Members of $\mathbb{Z}_n$ can be added and multiplied as follows: the sum $a +_n b$ of two members of $\mathbb{Z}_n$ is the ordinary sum $a + b$, reduced modulo $n$. (Precisely: To reduce an integer $x$ modulo $n$ is to write $x = nq + r$, with $q, r \in \mathbb{Z}$, and $0 \leq r < n$, and then write $r$ instead of $x$. So, for example, the result of reducing 23 modulo 10 is 3, the result of reducing 17 modulo 12 is 5, the result of reducing 17 modulo 7 is 3.) And the product $a \times_n b$ of two members of $\mathbb{Z}_n$ is the ordinary product $a \times b$ reduced modulo $n$.

So, for example,

$$
\begin{align*}
11 +_ {12} 12 & = 10 \\
18 +_ {22} 16 & = 12, \\
7 \times_9 8 & = 2, \\
2 \times_3 2 & = 1.
\end{align*}
$$

It is also common to write “$a + b$ modulo $n$”, or “$a + b$ mod $n$”, instead of “$a +_n b$”, and to write “$ab$ modulo $n$”, or “$ab$ mod $n$” (or “$a \times b$ modulo $n$”, or “$a \times b$ mod $n$”) instead of “$a +_n b$”, and “$a \times_n b$”. So, for example,

$$
\begin{align*}
11 + 12 & = 10 \mod 13, \\
18 + 16 & = 12 \mod 22, \\
7 \times 8 & = 2 \mod 9, \\
2 \times 2 & = 1 \mod 3.
\end{align*}
$$

An inverse modulo $n$ of a member $x$ of $\mathbb{Z}_n$ (also called an “inverse of $x$ in $\mathbb{Z}_n$”) is a member $y$ of $\mathbb{Z}_n$ such that $xy = 1$ modulo $n$. (For example, 8 is an inverse of 7 modulo 11, because $7 \times 8 = 56$, and 56, reduced modulo 11, is 1, so $7 \times 8 = 1$ modulo 11.)

1. Prove that if $p$ is a prime number then every nonzero member of $\mathbb{Z}_p$ has an inverse modulo $p$. (For example, let us take $p = 7$. Then $\mathbb{Z}_7$ has seven members, namely, 0, 1, 2, 3, 4, 5 and 6. The nonzero members of $\mathbb{Z}_7$ are 1, 2, 3, 4, 5 and 6. Then
$1 \times 1 = 1 \mod 7$, so 1 is an inverse of 1 modulo 7,  
$4 \times 2 = 1 \mod 7$, so 4 is an inverse of 2 modulo 7,  
$5 \times 3 = 1 \mod 7$, so 5 is an inverse of 3 modulo 7,  
$2 \times 4 = 1 \mod 7$, so 2 is an inverse of 4 modulo 7,  
$3 \times 5 = 1 \mod 7$, so 3 is an inverse of 5 modulo 7,  
$6 \times 6 = 1 \mod 7$, so 6 is an inverse of 6 modulo 7.

So we see that every nonzero member of $\mathbb{Z}_5$ has an inverse in $\mathbb{Z}_5$.)

(HINT: If $p$ is prime and $a$ is an arbitrary member of $\mathbb{Z}_p$ such that $a \neq 0$, show first that the greatest common divisor of $p$ and $a$ is 1; then use Bézout’s lemma to write $1 = up + va$, with $u, v$ integers; then write $v = qp + r$ with $q, r \in \mathbb{Z}$, and $0 \leq r < p$; finally, show that $ra = 1$ modulo $p$, so $r$ is an inverse of $a$ modulo $p$.)

2. Find

   i. an inverse of 11 in $\mathbb{Z}_{17}$,
   ii. an inverse of 42 in $\mathbb{Z}_{101}$.
   iii. an inverse of 33 in $\mathbb{Z}_{89}$.

3. Show that 5 does not have an inverse in $\mathbb{Z}_{10}$.

\footnote{Do not forget about Footnote 1!}
\footnote{This does not contradict the result of Part 1, because 10 is not prime.}