Number Theory – HW 1 – Due September 19

Problem 1 *By using Euclidean algorithm, find the g.c.d. of 2947 and 3997.*

Solution.

$$\begin{aligned}
\underbrace{3997}_{r_0} &= 1 * \underbrace{2947}_{r_1} + \underbrace{1050}_{r_2} \\
\underbrace{2947}_{r_1} &= 2 * \underbrace{1050}_{r_2} + \underbrace{847}_{r_3} \\
\underbrace{1050}_{r_2} &= 1 * \underbrace{847}_{r_3} + \underbrace{203}_{r_4} \\
\underbrace{847}_{r_3} &= 4 * \underbrace{203}_{r_4} + \underbrace{35}_{r_5} \\
\underbrace{203}_{r_4} &= 5 * \underbrace{35}_{r_5} + \underbrace{28}_{r_6} \\
\underbrace{35}_{r_5} &= 1 * \underbrace{28}_{r_6} + \underbrace{7}_{r_7} \\
\underbrace{28}_{r_6} &= 4 * \underbrace{7}_{r_7} + \underbrace{0}_{r_8}
\end{aligned}$$

$$\begin{aligned}
gcd(2947, 3997) &= (r_7, r_8) \\
&= (7, 0) \\
&= 7
\end{aligned}$$

Problem 2 *Find the g.c.d. d of the number 1819 and 3587, and then find integers x and y such that*

$$1819x + 3587y = d.$$

Solution.

$$\begin{aligned}
\underbrace{3587}_{r_0} &= 1 * \underbrace{1819}_{r_1} + \underbrace{1768}_{r_2} \\
\underbrace{1819}_{r_1} &= 1 * \underbrace{1768}_{r_2} + \underbrace{51}_{r_3} \\
\underbrace{1768}_{r_2} &= 34 * \underbrace{51}_{r_3} + \underbrace{34}_{r_4} \\
\underbrace{51}_{r_3} &= 1 * \underbrace{34}_{r_4} + \underbrace{17}_{r_5} \\
\underbrace{34}_{r_4} &= 2 * \underbrace{17}_{r_5} + \underbrace{0}_{r_6}
\end{aligned}$$

So $gcd(3587, 1819) = gcd(r_5, r_6) = gcd(17, 0) = 17.$

Learning outcomes:

Next, $2 * 1819 - 1 * 3587 = 51$. *Note that* $3587 = 70 * 51 + 17$.

$$\begin{aligned} 3587 &= 70 * 51 + 17 \\ 3587 &= 70 * (2 * 1819 - 3587) + 17 \\ -140 * 1819 + 71 * 3587 &= 17 \\ -140 * 1819 + 71 * 3587 &= gcd(3587, 1819) \end{aligned}$$

so $x = -140$, $y = 71$.

Problem 3 *Find values x and y to satisfy* $43x + 64y = 1$.

Left for you!

Problem 4 *Prove that if* n *is odd then* $n^2 - 1$ *is divisible by 8.*

Solution.

If n *is odd, we can write* $n = 2k + 1$ *for some* $k \in \mathbb{Z}$. *We have*

$$\begin{aligned} n^2 - 1 &= (2k+1)^2 - 1 \\ &= (4k^2 + 4k + 1) - 1 \\ &= 4k^2 + 4k \\ &= 4k(k+1). \end{aligned}$$

Either k *or* $k + 1$ *is even, so we can factor our 2 from one of these terms to get*

$$4k(k+1) = 8c,$$

for some $c \in \mathbb{Z}$. *Since* $8c = n^2 - 1$, $n^2 - 1$ *is divisible by 8 by definition.*

Problem 5 *Prove that any set of integers that are relatively prime in pairs are relatively prime.*

Solution.

Suppose we have n *distinct integers* $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. *Given that*

$$gcd(a_i, a_j) = 1 \tag{1}$$

for $i \neq j$, *if we consider the prime factorizationa*

$$a_k = \prod_p p^{\alpha_k(p)}, 1 \leq k \in \mathbb{N} \leq n,$$

Then $\min(\alpha_i(p), \alpha_j(p)) = 0$ *for all prime* p. *We prove that the set of numbers is relatively prime by contradiction. Suppose, they are not relatively prime. Then*

$$gcd(a_1, a_2, \ldots, a_n) \neq 1.$$

This implies that

$$min(\alpha_1(p), \alpha_2(p), \ldots, \alpha_n(p)) \neq 0$$

for some prime p. From this we have,

$$\alpha_k(p) \geq 1$$

for all $1 \leq k \leq n$ for some p. Therefore

$$min(\alpha_i(p), \alpha_j(p)) \geq 1 \tag{2}$$

for all i, j given some prime p. This contradicts equation 1. Therefore,

$$gcd(a_1, a_2, \ldots, a_n) = 1$$

Solution 2:

Suppose directly that $gcd(a_1, a_2, \ldots, a_n) = d \geq 1$. For $1 \leq i < j \leq n$, $d \mid a_i,\ a_j$. So, $d \mid gcd(a_i, a_j) = 1$. So, d must equal to 1. This completes the proof.

Problem 6 *Prove that if an integer is of the form $6k + 5$, then it is necessarily of the form $3\ell - 1$, but not conversely.*

Solution.

Regardless of the value of k, it is easy to see that $6k + 5 \equiv 1 \mod 2$. Thus, we can write odd numbers of the form $6k + 5$. If we can also write that number in the form $3k' - 1$, then

$$\begin{aligned} 3k' - 1 &\equiv 1 \mod 2 \\ 3k' &\equiv 2 \mod 2 \\ 3k' &\equiv 0 \mod 2 \\ k' &\equiv 0 \mod 2, \end{aligned}$$

so k' is even. Now we try to find a formula for k in terms of k' if a number can be written in both forms. We have

$$\begin{aligned} 6k + 5 &= 3k' - 1 \\ 6k - 3k' &= -6 \\ 3(2k - k') &= -6 \\ 2k - k' &= -2 \\ k &= \frac{k' - 2}{2}. \end{aligned}$$

Since k' is even, the term on the right is an integer. Thus, if a number can be written in the form $6k + 5$, we can substitute $k = \dfrac{k' - 2}{2}$ to recover the form $3k' - 1$.

Problem 7 *Prove that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3. Prove that an integer is divisible by 3 if and only if the sum of its digits is divisible by 9.*

Solution is given in class.

Problem 8 *Evaluate $gcd(ab, p^4)$ and $gcd(a + b, p^4)$ given that $gcd(a, p^2) = p$ and $gcd(b, p^3) = p^2$ where p is prime.*

Solution.

In this proof I use the fact that if $gcd(a, b) = d$ *and* $gcd(a, c) = 1$ *then* $gcd(a, bc) = d$*. I also use the notation* $p^e \parallel a$ *for a prime* p *and* $e, a \in \mathbb{Z}$ *to mean that* e *is the highest power of* p *that divides* a*.*

It is clear that from $gcd(a, p^2) = p$ *that* $p \parallel a$*. Thus,* $np = a$ *for some* $n \in \mathbb{Z}$ *where* $gcd(n, p) = 1$*.*

Likewise, from $gcd(b, p^3) = p^2$ *we see that* $p^2 \parallel b$*. Thus,* $mp^2 = b$ *for some* $m \in \mathbb{Z}$ *where* $gcd(m, p^2) = 1$*. This also implies* $gcd(m, p) = 1$*.*

Now we can prove $gcd(ab, p^4) = p^3$*. We know that*

$$gcd(p^4, p^3) = p^3. \tag{3}$$

Since $gcd(p, n) = 1$ *and* $gcd(p, m) = 1$*,* $gcd(p, nm) = 1$ *and therefore*

$$gcd(p^4, nm) = 1. \tag{4}$$

Combining equations 3 and 4 we get

$$\begin{aligned} gcd(p^4, mnp^3) &= 1 \\ gcd(p^4, ab) &= 1 \\ gcd(ab, p^4) &= 1 \end{aligned}$$

Now we aim to prove that $gcd(a + b, p^4) = p$*. We start with* $gcd(n + mp, p)$*. Clearly this gcd is equal to 1 or* p*. If the gcd is* p*, then* $p \mid n + mp$*. Since* $p \mid mp$*, then* $p \mid n$*. But* $gcd(n, p) = 1$*, so* $p \nmid n$*. Thus, the gcd is 1 so*

$$gcd(p^4, n + mp) = 1 \tag{5}$$

Clearly,

$$gcd(p^4, p) = p \tag{6}$$

Combining equations 5 and 6, we have

$$\begin{aligned} gcd(p^4, p(n + mp)) &= p \\ gcd(p^4, pn + mp^2) &= p \\ gcd(p^4, a + b) &= p \\ gcd(a + b, p^4) &= p \end{aligned}$$

Problem 9 *Find an integer* n *such that* $n/2$ *is a square,* $n/3$ *is a cube, and* $n/5$ *is a fifth power.*

Solution.

From the description of n*, we see that*

$$n = 2a^2 = 3b^3 = 5c^5,$$

for some $a, b, c \in \mathbb{Z}^+$*. Consider the prime factorization of* n*,*

$$n = \prod_p p^{\alpha(p)} a$$

for primes p*. We see that*

$$\begin{aligned} \alpha(2) &\equiv 1 \mod 2 \\ \alpha(2) &\equiv 0 \mod 3 \\ \alpha(2) &\equiv 0 \mod 5 \end{aligned}$$

The solution is $\alpha(2) \equiv 15 \mod 30$*.*

Likewise,

$$\begin{aligned}\alpha(3) &\equiv 0 \mod 2\\ \alpha(3) &\equiv 1 \mod 3\\ \alpha(3) &\equiv 0 \mod 5\end{aligned}$$

The solution is $\alpha(3) \equiv 10 \mod 30$.

Finally,

$$\begin{aligned}\alpha(5) &\equiv 0 \mod 2\\ \alpha(5) &\equiv 0 \mod 3\\ \alpha(5) &\equiv 1 \mod 5\end{aligned}$$

The solution is $\alpha(5) \equiv 6 \mod 30$.

By guess and check, the factorization

$$n = 2^{15} \cdot 3^{10} \cdot 5^{6}$$

is a solution.

Problem 10 *Prove that* $gcd(a^2, b^2) = d^2$ *if* $gcd(a, b) = d$.

Solution.

We aim to prove that $gcd(a^2, b^2) = c^2 \iff gcd(a, b) = c$. *Let*

$$a = \prod_p p^{\alpha(p)}$$
$$b = \prod_p p^{\beta(p)}$$

$(\longleftarrow)$
We see that

$$c = \prod_p p^{min(\alpha(p),\beta(p))}$$

Clearly,

$$\begin{aligned}a^2 &= \left(\prod_p p^{\alpha(p)}\right)^2\\ &= \prod_p \left(p^{\alpha(p)}\right)^2\\ &= \prod_p p^{2\alpha(p)},\end{aligned}$$

and

$$\begin{aligned}b^2 &= \left(\prod_p p^{\beta(p)}\right)^2\\ &= \prod_p \left(p^{\beta(p)}\right)^2\\ &= \prod_p p^{2\beta(p)}.\end{aligned}$$

Let $c' = \gcd(a^2, b^2)$. *Then*

$$c' = \prod_p p^{min(2\alpha(p),2\beta(p))}.$$

But

$$\begin{aligned} c^2 &= \left(\prod_p p^{min(\alpha(p),\beta(p))}\right)^2 \\ &= \prod_p \left(p^{min(\alpha(p),\beta(p))}\right)^2 \\ &= \prod_p p^{2\cdot min(\alpha(p),\beta(p))} \\ &= \prod_p p^{min(2\alpha(p),2\beta(p))}. \end{aligned}$$

so $c^2 = c'$ *and* $\gcd(a,b) = c$ *implies* $\gcd(a^2, b^2) = c^2$.

($\longrightarrow$)
To prove the converse, assuming $\gcd(a^2, b^2) = c^2$, *we simply reverse the steps for how we calculated* a^2, b^2 *and* c^2 *to get formulas for* a, b, c. *We know that* $\gcd(a,b) = \prod_p p^{min(\alpha(p),\beta(p))}$, *which is equal to* c, *so* $c = \gcd(a,b)$.

Problem 11 *Determine whether the following assertions are true or false. If true, prove the result. If false, give a counterexample.*

(a) *If* $(a,b) = (a,c)$ *then* $[a,b] = [a,c]$.

Solution: *Picking* $a = 2,\ b = 3,\ c = 5$, *we get* $(a,b) = 1 = (a,c)$ *but* $[a,b] = 6 \neq 10[a,c]$. *So, the statement is false!*

(b) *If* $(a,b) = (a,c)$ *then* $(a^2, b^2) = (a^2, c^2)$.

(c) *If* $(a,b) = (a,c)$ *then* $(a,b,c) = (a,b)]$.

(d) *If* p *is prime,* $p|a$ *and* $p|(a^2 + b^2)$ *then* $p|b$.

(e) *If* p *is prime and* $p|a^7$ *then* $p|a$.

(f) *If* $a^3|c^3$ *then* $a|c$.

(g) *If* $a^3|c^2$ *then* $a|c$.

(h) *If* $a^2|c^3$ *then* $a|c$.

(i) *If* p *is prime,* $p|(a^2 + b^2)$ *and* $p|(b^2 + c^2)$, *then* $p|(a^2 - c^2)$.

(j) *If* p *is prime,* $p|(a^2 + b^2)$ *and* $p|(b^2 + c^2)$, *then* $p|(a^2 + c^2)$.

(k) *If* $(a,b) = 1$ *then* $(a^2, ab, b^2) = 1$.

(l) $[a^2, ab, b^2] = [a^2, b^2]$.

(m) *If* $b|(a^2 + 1)$, *then* $b|(a^4 + 1)$.

(n) *If* $b|(a^2 - 1)$, *then* $b|(a^4 - 1)$.

(o) $(a,b,c) = ((a,b),(a,c))$.

Solution: *(Throughout the following proof, we use the definition of gcd implicitly without mentioning.) Let* $d = (a,b,c)$. *Let* $g = ((a,b),(a,c))$ *Then* $d \mid a,\ b,\ c$. *This implies* $d \mid (a,b),\ (a,c)$. *Hence,* $d \mid ((a,b),(a,c)) = g$. *Conversely,* $g \mid (a,b),\ (a,c)$. *This implies* $g \mid a,\ b$ *and* $g \mid a,\ c$. *When combined,* $g \mid a,\ b,\ c$. *So,* $g \mid (a,b,c) = d$. *Since* $d \mid g$ *and* $g \mid d$, *we get that* $g = d$.