Soluitions to Homework 7

Solution to 25d). First we find a primitive root modulo 17. It is not hard to see that that 3 is a primitive root modulo 17. Indeed, the order of 3 modulo 17 divides 16. We have $3^2 \equiv -8 = -2^3 (\mod 17)$ so $3^8 \equiv 2^{12} = (2^4)^3 \equiv -1 (\mod 17)$. It follows that order of 3 modulo 17 does not divide 8, hence it must be equal to 16.

Now $3^{16} - 1 = (3-1)(3+1)(3^2+1)(3^4+1)(3^8+1)$ is not divisible by 17^2 so 3 is a primitive root modulo every power of 17 (if $3^{16}-1$ was divisible by 17^2, we would replace 3 by $3+17=20$). Since 3 is odd, it is also a primitive root modulo $2 \cdot 17^m$.

Here is a different solution. It is not hard to see that 6 is also a primitive root modulo 17 and 17^2 does not divide $6^{16}-1$. Thus 6 is a primitive root modulo any power of 17. However 6 is even, so to get a primitive root modulo $2 \cdot 17^m$ we use $6+17^2$, which is odd.

Finally, let us remark that if p is an odd prime there is always an odd integer a which is a primitive root modulo p and such that $a^{p-1}-1$ is not divisible by p^2. Such a is a primitive root modulo p^m and modulo $2p^m$ for every m.

Problem 28a). When $m=2$ the result is obvious. Assume now that $m>2$, so $\phi(m)$ is even. Suppose that a is a primitive root modulo m. Then
$a^{\phi(m)/2} \equiv -1 (\mod m)$. Indeed, we have $-1 \equiv a^k (\mod m)$ for some (unique) k such that $0 \le k < \phi(m)$. But then $a^{2k} \equiv 1 (\mod m)$, so $\phi(m)$ divides $2k$ and therefore $\phi(m)/2$ divides k. The only positive k less than $\phi(m)$ and divisible by $\phi(m)/2$ is $k = \phi(m)/2$. We proved the following:

If a is a primitive root modulo $m>2$ then $\mathrm{ind}_a(-1) = \phi(m)/2$.

Since a is a primitive root modulo m, the numbers $a^0, a^1, \ldots, a^{\phi(m)-1}$ taken modulo m give all the residues modulo m which are relatively prime to m. Thus the product of all the positive integers less than m and relatively prime to m is congruent modulo m to the product

$$a^0 a^1 \ldots a^{\phi(m)-1} = a^{1+2+\ldots+(\phi(m)-1)} = a^{(\phi(m)-1)\phi(m)/2} =$$
$$= (a^{\phi(m)/2})^{\phi(m)-1} \equiv (-1)^{\phi(m)-1} = -1 (\mod m)$$

(in the last step we used the fact that $\phi(m)-1$ is odd.)

Solution to Problem 32c). We know that 3 is a primitive root modulo 17. Thus x is a solution to $8x^{12} \equiv b (\mod 17)$ if and only if

$$\mathrm{ind}_3(8) + 12\mathrm{ind}_3(x) \equiv \mathrm{ind}_3(b) \pmod{16} .$$

Now, since $8 \equiv -9 \pmod{17}$, we have

$$\mathrm{ind}_3(8) = \mathrm{ind}_3(-3^2) \equiv \mathrm{ind}_3(-1) + \mathrm{ind}_3(3^2) = 8+2 = 10 \pmod{16} .$$

Thus $\mathrm{ind}_3(8) = 10$. We used the fact from problem 28a) which yields $\mathrm{ind}_3(-1) = 8$.

It follows that our original congruence is solvable if and only if the congruence $10 + 12y \equiv \mathrm{ind}_3(b) \pmod{16}$ is solvable, i.e. when $12y \equiv \mathrm{ind}_3(b) - 10 \pmod{16}$ is solvable. This happens if and only if $\gcd(12,16) = 4$ divides $\mathrm{ind}_3(b) - 10$. Among the possible choices $0, 1, \ldots, 15$ for $\mathrm{ind}_3(b)$ only $2, 6, 10, 14$ have this property. Thus our congruence is solvable if and only if $\mathrm{ind}_3(b)$ is one of $2, 6, 10, 14$. Note that
$3^4 \equiv -4 \pmod{17}$. Thus

$$3^6 = 3^2 \cdot 3^4 \equiv 9(-4) = -36 \equiv 15 \equiv -2 \pmod{17} ,$$

$$3^{10} = 3^6 \cdot 3^4 \equiv (-2)(-4) = 8 \pmod{17} ,$$

and

$$3^{14} = 3^{10} \cdot 3^4 \equiv 8(-4) = -32 \equiv 2 \pmod{17} .$$

Thus our congruence is solvable if and only if b is congruent to one of $2, 8, 9, 15$ modulo 17.

Solution to problem 35. a) Since s, r are primitive roots modulo a prime p, we have $r \equiv s^{\mathrm{ind}_s(r)} \pmod{p}$. Thus

$$a \equiv r^{\mathrm{ind}_r(a)} \equiv (s^{\mathrm{ind}_s(r)})^{\mathrm{ind}_r(a)} = s^{\mathrm{ind}_s(r)\mathrm{ind}_r(a)} \pmod{p} .$$

This means that $\mathrm{ind}_s(a) \equiv \mathrm{ind}_s(r)\mathrm{ind}_r(a) \pmod{p-1}$ (as $\phi(p) = p-1$).

b) We have proved in the solution to Problem 28a) that if $m > 2$ and a is a primitive root modulo m then $\mathrm{ind}_a(-1) \equiv \phi(m)/2 \pmod{\phi(m)}$. Thus

$$\mathrm{ind}_r(p-a) \equiv \mathrm{ind}_r(-a) \equiv \mathrm{ind}_r(-1) + \mathrm{ind}_r(a) \equiv \frac{p-1}{2} + \mathrm{ind}_r(a) \pmod{p-1} .$$

Solution to Problem 38. Since the set $\{1^n, 2^n, \ldots, (p-1)^n\}$ contains $p-1$ numbers, each relatively prime to p, it suffices to show that no two of these numbers are congruent modulo p. Let r be a primitive root modulo p and $1 \le a, b < p$. Then $a^n \equiv b^n \pmod{p}$ if and only if $\mathrm{ind}_r(a^n) \equiv \mathrm{ind}_r(b^n) \pmod{p-1}$, i.e. if and only if $n\mathrm{ind}_r(a) \equiv n\mathrm{ind}_r(b) \pmod{p-1}$. Since n is relatively prime to $p-1$, the last congruence is equivalent to $\mathrm{ind}_r(a) \equiv \mathrm{ind}_r(b) \pmod{p-1}$ which is the same as $a \equiv b \pmod{p}$. This proves that our numbers are indeed all different modulo p and therefore they form a reduced residue system modulo p.

Here is a different argument that if $a^n \equiv b^n \pmod{p}$ then $a \equiv b \pmod{p}$. Since n is relatively prime to $p-1$, there is an integer $k > 0$ such that $kn \equiv 1 \pmod{p-1}$. Now $a^n \equiv b^n \pmod{p}$ implies that $a^{kn} \equiv b^{kn} \pmod{p}$. On the other hand, since $kn \equiv 1 \pmod{p-1}$, we have $a^{kn} \equiv a \pmod{p}$ and $b^{kn} \equiv b \pmod{p}$. Thus $a \equiv b \pmod{p}$.

Problem 1. Let p be an odd prime number. Let a, b be integers such that $a \equiv b \pmod{p}$ and $\gcd(a, p) = 1$. Prove that

$$a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv p \pmod{p^2} .$$

Solution. We show three ways to solve the problem. Our first solution uses the result from class, where we proved the result for $b = 1$. Let d be an inverse of a modulo p^2, so $ad \equiv 1 \pmod{p^2}$. Since $a \equiv b \pmod{p}$, we have $bd \equiv ad \equiv 1 \pmod{p}$. Thus $1 + (bd) + \ldots + (bd)^{p-1} \equiv p \pmod{p^2}$ by the result from class. Multiplying the last congruence by a^{p-1} and observing that

$$(bd)^i a^{p-1} = b^i a^{p-1-i}(ad)^i \equiv b^i a^{p-1-i} \pmod{p^2}$$

we get

$$a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv pa^{p-1} \pmod{p^2} .$$

Since $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem, we see that $pa^{p-1} \equiv p \pmod{p^2}$. Thus $a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv p \pmod{p^2}$.

Our second solution extends the method from class (the case when $b = 1$). Since $a \equiv b \pmod{p}$, we have $a^i b^j \equiv a^{i+j} \pmod{p}$ for any non-negative integers i, j. It follows that

$$a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1} \equiv ka^{k-1} \pmod{p}$$

for any integer $k > 0$. Since p divides $a - b$, multiplying the last congruence by $a - b$ yields

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \ldots + ab^{k-2} + b^{k-1}) \equiv ka^{k-1}(a-b) \pmod{p^2}$$

i.e.

$$b^k \equiv a^k - ka^{k-1}(a-b) \pmod{p^2}$$

(note that we get a congruence modulo p^2). Multiplying by a^{p-1-k} we get

$$a^{p-1-k}b^k \equiv a^{p-1} - ka^{p-2}(a-b) \pmod{p^2} .$$

Adding these congruences for $k = 0, 1, \ldots, p-1$, we get

$$a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv pa^{p-1} - a^{p-2}(a-b)(0 + 1 + \ldots + (p-1)) \pmod{p^2} .$$

Now $0 + 1 + \ldots + (p-1) = (p-1)p/2$ is divisible by p and so is $a - b$, so $a^{p-2}(a-b)(0 + 1 + \ldots + (p-1) \equiv 0 \pmod{p^2}$. Thus

$$a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv pa^{p-1} \pmod{p^2} .$$

As noticed in our first solution, $pa^{p-1} \equiv p \pmod{p^2}$, so $a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} \equiv p \pmod{p^2}$.

Our third solution will use the binomial theorem and the fact that when p is a prime number then $\binom{p}{i}$ is divisible by p for $i = 1, 2, \ldots, p-1$. From $a \equiv b \pmod{p}$ we see that $a = b + kp$ for some integer k. Thus

$$a^p = (b+kp)^p = b^p + \binom{p}{1}b^{p-1}kp + \binom{p}{2}b^{p-2}(kp)^2 + \ldots + \binom{p}{p-1}b(kp)^{p-1} + (kp)^p.$$

Note that each term in the sum on the right hand side, starting from the third term, is divisible by kp^3. Thus we can write $a^p - b^p = kp(b^{p-1}p + lp^2)$ for some integer l. Since

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1}) = kp(a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1})$$

we conclude that

$$a^{p-1} + a^{p-2}b + \ldots + ab^{p-2} + b^{p-1} = b^{p-1}p + lp^2 \equiv b^{p-1}p \equiv p \pmod{p^2}$$

(we used again the observation from our first solution that $pb^{p-1} \equiv p \pmod{p^2}$).

Problem 2. Let p be an odd prime and let a, b be integers not divisible by p. In this problem we study the highest power of p which divides $a^n - b^n$ for positive integers n. Let m be the smallest positive integer such that $p|(a^m - b^m)$ and let p^s be the highest power of p which divides $a^m - b^m$ (so $s = e_p(a^m - b^m)$).

a) Let c be the inverse of b modulo p, so $bc \equiv 1 \pmod{p}$. Prove that $m = \mathrm{ord}_p(ac)$.

b) Prove that if $m \nmid n$ then $p \nmid a^n - b^n$.

From now on suppose that $m|n$. Thus we can factor $n = mp^k N$ for some $k \geq 0$ and some N not divisible by p.

c) Show that p^s is the highest power of p which divides $a^{mN}-b^{mN}$ (i.e. $e_p(a^{mN}-b^{mN})=s$).

d) Use Problem 1 and induction on r to show that p^{s+r} is the highest power of p which divides $a^{mNp^r}-b^{mNp^r}$. Conclude that

$$e_p(a^n-b^n)=\begin{cases}0 & \text{if } m\nmid n\\ e_p(a^m-b^m)+e_p(n) & \text{if } m|n.\end{cases}$$

e) Find and prove a similar formula for $e_2(a^n-b^n)$ for odd integers a,b.

Solution. a) Note that p divides a^k-b^k if and only if $a^k\equiv b^k \pmod p$, which is equivalent to $c^ka^k\equiv c^kb^k=(cb)^k\equiv 1 \pmod p$. Thus m is the smallest positive integer such that $c^ka^k=(ac)^k\equiv 1 \pmod p$, i.e. $m=\mathrm{ord}_p(ac)$.

b) We have seen in a) that p divides a^n-b^n if and only if $(ac)^n\equiv 1 \pmod p$, which holds if and only if $m|n$. Thus if $m\nmid n$ then $p\nmid(a^n-b^n)$, i.e. $e_p(a^n-b^n)=0$.

c) We have

$$a^{mN}-b^{mN}=(a^m-b^m)\left((a^m)^{N-1}+(a^m)^{N-2}(b^m)+(a^m)^{N-3}(b^m)^2+\ldots+(a^m)(b^m)^{N-2}+(b^m)^{N-1}\right).$$

Since $a^m\equiv b^m \pmod p$, for every $i=0,\ldots,N-1$ we have

$$(a^m)^{N-1-i}(b^m)^i\equiv(a^m)^{N-1-i}(a^m)^i=(a^m)^{N-1} \pmod p .$$

It follows that

$$(a^m)^{N-1}+(a^m)^{N-2}(b^m)+(a^m)^{N-3}(b^m)^2+\ldots+(a^m)(b^m)^{N-2}+(b^m)^{N-1}\equiv N(a^m)^{N-1} \pmod p .$$

In particular, the number $(a^m)^{N-1}+(a^m)^{N-2}(b^m)+(a^m)^{N-3}(b^m)^2+\ldots+(a^m)(b^m)^{N-2}+(b^m)^{N-1}$ is not divisible by p and therefore the highest power of p which divides $a^{mN}-b^{mN}$ is the same as the highest power of p which divides a^m-b^m. In other words, $e_p(a^{mN}-b^{mN})=s=e_p(a^m-b^m)$.

d) Note that Problem 1 tells us that if A,B are integers not divisible by p and $A\equiv B \pmod p$ then $e_p(A^{p-1}+A^{p-2}B+\ldots+AB^{p-2}+B^{p-1})=1$. We prove by induction on r that $e_p(a^{mNp^r}-b^{mNp^r})=s+r$. In part c) we showed it for $r=0$. Suppose that the formula is true for some $r\geq 0$. Let $A=a^{mNp^r}$ and $B=b^{mNp^r}$. Then $A\equiv B \pmod p$, $e_p(A-B)=s+r$ and

$$a^{mNp^{r+1}}-b^{mNp^{r+1}}=A^p-B^p=(A-B)(A^{p-1}+A^{p-2}B+\ldots+AB^{p-2}+B^{p-1}).$$

Thus

$$e_p(a^{mNp^{r+1}}-b^{mNp^{r+1}})=e_p((A-B)(A^{p-1}+A^{p-2}B+\ldots+AB^{p-2}+B^{p-1}))=$$

$$e_p(A-B)+e_p(A^{p-1}+A^{p-2}B+\ldots+AB^{p-2}+B^{p-1})=r+s+1.$$

This proves that the formula is true for $r+1$. By the method of mathematical induction, the formula is true for all integers $r\geq 0$.

Note that p does not divide m (since $m=\mathrm{ord}_p(ac)$ divides p-1). Thus $k=e_p(n)$. Taking $r=k$ in our formula, we see that $e_p(a^n-b^n)=s+k=e_p(a^m-b^m)+e_p(n)$.

e) Let $n = 2^k N$, where N is odd and $k \geq 0$. We have

$$a^N - b^N = (a-b)(a^{N-1} + a^{N-2}b + a^{N-3}b^2 + \ldots + ab^{N-2} + b^{N-1}).$$

The second factor is a sum of an odd number of odd numbers, so it is odd. It follows that $e_2(a^N - b^N) = e_2(a-b)$. Similarly,

$$a^N + b^N = (a+b)(a^{N-1} - a^{N-2}b + a^{N-3}b^2 - \ldots - ab^{N-2} + b^{N-1})$$

and the second factor is odd, so $e_2(a^N + b^N) = e_2(a+b)$. Suppose now that $k \geq 1$. Then

$$a^n - b^n = (a^N - b^N)(a^N + b^N)((a^N)^2 + (b^N)^2)\ldots((a^N)^{2^{k-1}} + (b^N)^{2^{k-1}}).$$

Recall now that if A, B are odd then $e_2(A^2 + B^2) = 1$. It follows that

$$e_2(a^n - b^n) = e_2((a^N - b^N)(a^N + b^N)((a^N)^2 + (b^N)^2)\ldots((a^N)^{2^{k-1}} + (b^N)^{2^{k-1}})) = e_2(a^N - b^N) + e_2(a^N + b^N) +$$

$$e_2((a^N)^2 + (b^N)^2) + \ldots + e_2((a^N)^{2^{k-1}} + (b^N)^{2^{k-1}}) = e_2(a-b) + e_2(a+b) + k - 1.$$

Since $k = e_2(n)$, we can summarize our results as follows:

$$e_2(a^n - b^n) = \begin{cases} e_2(a-b) & \text{if } e_2(n) = 0 \\ e_2(a-b) + e_2(a+b) + e_2(n) - 1 & \text{if } e_2(n) \geq 1. \end{cases}$$

Problem 3. Let p, q, r be three distinct prime numbers. Prove that

$$(pq)^{r-1} + (pr)^{q-1} + (qr)^{p-1} \equiv 1 \pmod{pqr}\ .$$

Solution. The congruence

$$(pq)^{r-1} + (pr)^{q-1} + (qr)^{p-1} \equiv 1 \pmod{pqr}$$

is equivalent to three congruences

$$(pq)^{r-1} + (pr)^{q-1} + (qr)^{p-1} \equiv 1 \pmod{p}\ ,\ (pq)^{r-1} + (pr)^{q-1} + (qr)^{p-1} \equiv 1 \pmod{q}\ ,\ \text{and}$$

$$(pq)^{r-1} + (pr)^{q-1} + (qr)^{p-1} \equiv 1 \pmod{r}\ .$$

For the first congruence,

$$(pq)^{r-1} + (pr)^{q-1} + (qr)^{p-1} \equiv 0 + 0 + 1 = 1 \pmod{p}$$

(we used Fermat's Little theorem to get $(qr)^{p-1} \equiv 1 \pmod{p}$). Same argument justifies the other 2 congruences.

Problem 4. Let m, n be positive integers such that $m|n$. Prove that $\phi(m)|\phi(n)$ and $\phi(mn) = m\phi(n)$.

Solution. Write $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, where $p_1, \ldots, p_k$ are distinct prime numbers and $a_1, \ldots, a_k$ are positive integers. Since $m|n$, we have $n = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k} p_{k+1}^{b_{k+1}} \ldots p_{k+s}^{b_{k+s}}$, where $s \geq 0$, $p_{k+1}, \ldots p_{k+s}$ are distinct prime numbers different from $p_1, \ldots, p_k$, $b_i \geq a_i$ for $i = 1, \ldots, k$, and $b_i > 0$ for $i = k+1, \ldots, k+s$. Then

$$\phi(m) = (p_1 - 1)p_1^{a_1 - 1}(p_2 - 1)p_2^{a_2 - 1} \ldots (p_k - 1)p_k^{a_k - 1},$$

$$\phi(n) = (p_1 - 1)p_1^{b_1-1}(p_2 - 1)p_2^{b_2-1} \dots (p_k - 1)p_k^{b_k-1}(p_{k+1} - 1)p_{k+1}^{b_{k+1}-1} \dots (p_{k+s} - 1)p_{k+s}^{b_{k+s}-1},$$

and

$$\phi(mn) = (p_1-1)p_1^{a_1+b_1-1}(p_2-1)p_2^{a_2+b_2-1} \dots (p_k-1)p_k^{a_k+b_k-1}(p_{k+1}-1)p_{k+1}^{b_{k+1}-1} \dots (p_{k+s}-1)p_{k+s}^{b_{k+s}-1} =$$

$$m\phi(n).$$

The last equality proves the second part of the problem. The first two equalities give us

$$\phi(n) = \phi(m)p_1^{b_1-a_1}p_2^{b_2-a_2} \dots p_k^{b_k-a_k}(p_{k+1} - 1)p_{k+1}^{b_{k+1}-1} \dots (p_{k+s} - 1)p_{k+s}^{b_{k+s}-1}$$

so $\phi(m)|\phi(n)$.

Problem 5. Let m, n be relatively prime positive integers and let a be relatively prime to mn. Prove that $\text{ord}_{mn}a = \text{lcm}(\text{ord}_m a, \text{ord}_n a)$.

Solution. Let $k = \text{ord}_{mn}a$. Then $a^k \equiv 1 \pmod{mn}$. This implies $a^k \equiv 1 \pmod{m}$ and $a^k \equiv 1 \pmod{n}$, so $\text{ord}_m a|k$ and $\text{ord}_n a|k$. This implies that $\text{lcm}(\text{ord}_m a, \text{ord}_n a)|k$. On the other hand, since both $\text{ord}_m a|\text{lcm}(\text{ord}_m a, \text{ord}_n a)$ and $\text{ord}_n a|\text{lcm}(\text{ord}_m a, \text{ord}_n a)$ we have

$$a^{\text{lcm}(\text{ord}_m a, \text{ord}_n a)} \equiv 1 \pmod{m} \text{ and } a^{\text{lcm}(\text{ord}_m a, \text{ord}_n a)} \equiv 1 \pmod{n} .$$

Since $\gcd(m, n) = 1$, we conclude that

$$a^{\text{lcm}(\text{ord}_m a, \text{ord}_n a)} \equiv 1 \pmod{mn} .$$

This implies that $k|\text{lcm}(\text{ord}_m a, \text{ord}_n a)$. Earlier we showed that $\text{lcm}(\text{ord}_m a, \text{ord}_n a)|k$, so $\text{lcm}(\text{ord}_m a, \text{ord}_n a) = k$.

Problem 6. Let $p < q$ be odd prime numbers. Prove that pq is not a Carmichael number. Hint: Show first that there is an integer a which is a primitive root modulo p and a primitive root modulo q (use Chinese Reminder Theorem).

Solution. Since p and q are prime numbers, there exists integers b, c such that b is a primitive root modulo p and c is a primitive root modulo q. By the Chinese Remainder Theorem, there is an integer a such that $a \equiv b \pmod{p}$ and $a \equiv c \pmod{q}$. This means that a is a primitive root modulo p and a primitive root modulo q. If pq was a Carmichael number, we would have $a^{pq} \equiv a \pmod{pq}$. Since a is relatively prime to pq, we get $a^{pq-1} \equiv 1 \pmod{pq}$. Since $\text{ord}_q a = q - 1$, we see that $(q - 1)|pq - 1 = p(q - 1) + p - 1$. It follows that $(q - 1)|(p - 1)$, which contradicts the ineuqality $p < q$. The contradiction shows that pq is not a Carmichael number.

Problem 7. Let a, b, c be integers. Prove that

$$\text{lcm}(\gcd(a, b), \gcd(a, c)) = \gcd(a, \text{lcm}(b, c))$$

and

$$\text{lcm}(a, b, c) = \frac{abc \ \gcd(a, b, c)}{\gcd(a, b)\gcd(a, c)\gcd(b, c)}.$$

Hint: One approach is to verify this by evaluating e_p of each side for every prime p.

Solution. We will use the following useful facts:

(i) if m, n are positive integers then $m = n$ if and only if $e_p(m) = e_p(n)$ for every prime p.

(ii) $e_p(\text{lcm}(m, n)) = \max(e_p(m), e_p(n))$.

(iii) $e_p(\gcd(m, n)) = \min(e_p(m), e_p(n))$.

Now let p be a prime and let $k = e_p(a), l = e_p(b), m = e_p(c)$. Then $e_p(\gcd(a, b)) = \min(k, l)$, $e_p(\gcd(a, c)) = \min(k, m)$, $e_p(\gcd(b, c)) = \min(l, m)$, $e_p(\text{lcm}(b, c)) = \max(l, m)$, $e_p(\gcd(a, b, c)) = \min(k, l, m)$, and $e_p(\text{lcm}(a, b, c)) = \max(k, l, m)$ It follows that

$$e_p(\text{lcm}(\gcd(a, b), \gcd(a, c))) = \max(\min(k, l), \min(k, m))$$

and

$$e_p(\gcd(a, \text{lcm}(b, c))) = \min(k, \max(l, m)).$$

It is now a simple verification to see that $\max(\min(k, l), \min(k, m)) = \min(k, \max(l, m))$. Indeed, if $k \geq \max(l, m)$ then both sides are $\max(l, m)$ and if $k < \max(l, m)$ then both sides are equal to k. We proved that

$$e_p(\text{lcm}(\gcd(a, b), \gcd(a, c))) = e_p(\gcd(a, \text{lcm}(b, c)))$$

for every prime p, and therefore

$$\text{lcm}(\gcd(a, b), \gcd(a, c)) = \gcd(a, \text{lcm}(b, c)).$$

For the second euqality, which is symmetric in a, b, c, there is no loss in generality to assume that $k \geq l \geq m$. Then $e_p(\text{lcm}(a, b, c)) = k$, $e_p(\gcd(a, b, c)) = m$, $e_p(\gcd(a, b)) = l$, $e_p(\gcd(a, c)) = m$, $e_p(\gcd(b, c)) = m$ and

$$e_p\left(\frac{abc\ \gcd(a, b, c)}{\gcd(a, b)\gcd(a, c)\gcd(b, c)}\right) = (k + l + m) + m - (l + m + m) = k = e_p(\text{lcm}(a, b, c)).$$

We proved that

$$e_p\left(\frac{abc\ \gcd(a, b, c)}{\gcd(a, b)\gcd(a, c)\gcd(b, c)}\right) = e_p(\text{lcm}(a, b, c))$$

for every prime p and therefore

$$\frac{abc\ \gcd(a, b, c)}{\gcd(a, b)\gcd(a, c)\gcd(b, c)} = \text{lcm}(a, b, c).$$

Problem 8. Find the decimal expansion of $\dfrac{102}{10175}$ without using calculator.

Solution. For the results needed for this problem see solution to Quiz 7. We have $a = 102$, $b = 10175 = 5^2 \cdot 407 = 5^2 \cdot 11 \cdot 37$, $B = 407 = 11 \cdot 37$, $u = 0$, $w = 2$, $k = 2$. Since $10 \equiv -1 \pmod{11}$, we see that $\text{ord}_{11}10 = 2$. Recall that $10^3 - 1 = 3^3 \cdot 37$. It follows that $\text{ord}_{37}10 = 3$. From homework 7, Problem 5 we see that

$$\text{ord}_{407}10 = \text{lcm}(\text{ord}_{11}10, \text{ord}_{37}10) = \text{lcm}(2, 3) = 6.$$

Thus $s = 6$. The division algorithm yields

$$2^{k-u}5^{k-w}a = 4 \cdot 102 = 1 \cdot 407 + 1.$$

Thus $\alpha = 1$ and

$$\beta = 1 \cdot (10^6 - 1)/407 = (10^3 - 1)(10^3 + 1)/(11 \cdot 37) = 27 \cdot 91 = 2457.$$

Thus

$$\frac{102}{10175} = 0.01\overline{002457}.$$

Alternatively, one can perform the long division below, which stops when we get first time a repating division (in our case 250 repeats) and from it it follows that $s = 6, k = 2$ and

$$\frac{102}{10175} = 0.01\overline{002457}.$$

$$\begin{array}{rl}
102 & : \ 10157 \ = 0.01002457 \\
1020 & \\
10200 & \\
-\underline{10175} & \\
\quad 250 & \\
\quad 2500 & \\
\quad 25000 & \\
\quad -\underline{20350} & \\
\quad\quad 46500 & \\
\quad\quad -\underline{40700} & \\
\quad\quad\quad 58000 & \\
\quad\quad\quad -\underline{50875} & \\
\quad\quad\quad\quad 71250 & \\
\quad\quad\quad\quad -\underline{71225} & \\
\quad\quad\quad\quad\quad 250 &
\end{array}$$