Math 211

Assignment 4 - Solutions

[2] 1. Suppose $\sqrt[3]{40}$ were rational, so $\sqrt[3]{40} = \frac{m}{n}$ with $m, n \in \mathbb{Z}$. Then $40 = \frac{m^3}{n^3}$, or $40n^3 = m^3$. Thus $3\mathrm{expt}_5(m) = \mathrm{expt}_5(m^3) = \mathrm{expt}_5(40n^3) = \mathrm{expt}_5(40) + \mathrm{expt}_5(n^3) = 1 + 3\mathrm{expt}_5(n)$. We thus obtain that $1 + 3\mathrm{expt}_5(n) = 3\mathrm{expt}_5(m)$ which is impossible since 3 does not divide 1. Thus, no such integers m, n exist and hence $\sqrt[3]{40}$ is irrational.

Note: We could *not* have obtained a contradiction by using expt_2 (or expt_3) in place of expt_5. Similarly, an odd/even argument does not work here; instead, we need to discuss divisibility by 3.

[3] 2. (a) By the GCD-formula we have

$$\gcd(2^5 3^7 11^3 17^2, 3^2 5^3 7^4 13^2) = 2^{\min(5,0)} 3^{\min(7,2)} 5^{\min(0,3)} 7^{\min(0,4)} 11^{\min(3,0)} 13^{\min(0,2)} 17^{\min(2,0)} = 3^2.$$

(b) By the first part of Theorem 9 (GCD-formula), every divisor of $n = 3^2 5^3 7^4 13^2$ has the (unique) form

$$\pm 3^a 5^b 7^c 13^d, \quad \text{where } 0 \le a \le 2,\ 0 \le b \le 3,\ 0 \le c \le 4,\ 0 \le d \le 2.$$

Thus, there are $(2+1)(3+1)(4+1)(2+1) = 180$ positive divisors and 360 divisors in total. The first few are: $\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 13, \pm 15, \pm 21, \ldots$; these correspond to the values $(a, b, c, d) = (0,0,0,0), (1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (2,0,0,0), (1,1,0,0), (1,0,1,0)$, respectively.

(c) The prime decomposition of mn is $mn = 2^{5+0} 3^{7+2} 5^{0+3} 7^{0+4} 11^{3+0} 13^{0+2} 17^{2+0} = 2^5 3^9 5^3 7^4 11^3 13^2 17^2$.

[5] 3. (a) Since $2^{12} = (2^6)^2 = 64^2 \equiv 1^2 \equiv 1 \pmod{63}$, we have $\mathrm{rem}(2^{12}, 63) = 1$.

(b) Since $9 + 8 = 17$, we have $9 \equiv -8 \pmod{17}$, and so $9^5 \equiv (-8)^5 \pmod{17}$. But $(-8)^5 = -(8^5)$, so $9^5 \equiv -8^5 \pmod{17}$ or $9^5 + 8^5 \equiv 0 \pmod{17}$. Thus $\mathrm{rem}(8^5 + 9^5, 17) = 0$.

(c) Since $3^2 = 9 \equiv -1 \pmod{10}$, we have $3^8 = (3^2)^4 \equiv (-1)^4 \equiv 1 \pmod{10}$. Similarly, $4^8 = 16^4 \equiv (-4)^4 = 16^2 \equiv (-4)^2 \equiv 16 \equiv -4 \pmod{10}$. Thus, $3^8 - 4^8 \equiv 1 - (-4) \equiv 5 \pmod{10}$ and so $\mathrm{rem}(3^8 - 4^8, 10) = 5$.

(d) We have $24 \cdot 25 + 27 \cdot 29 \equiv (-2)(-1) + (1)(3) \equiv 5 \pmod{26}$, so $\mathrm{rem}(24 \cdot 25 + 27 \cdot 29, 26) = 5$.

(e) Here $103 \cdot 65 - 329 \cdot 663 \equiv 4(-1) - (-1)(3) \equiv -1 \equiv 32 \pmod{33}$, so $\mathrm{rem}(103 \cdot 65 - 329 \cdot 663, 33) = 32$.

[2] 4. We have $234785346 \equiv (2+3+4) + 7 + 8 + (5+4) + (3+6) \equiv 15 \equiv 6 \pmod 9$ and $5683592187 \equiv 5 + (6+3) + (8+1) + 5 + (9) + (2+7) + 8 \equiv 18 \equiv 0 \pmod 9$. Thus $234785346 \cdot 5683592187 \equiv 6 \cdot 0 \equiv 0 \pmod 9$. On the other hand, $1334424157147691702 \equiv (1+3+3+2) + (4+4+1) + (4+5) + (1+7+1) + 4 + 7 + 6 + (9) + 1 + (7+0+2) \equiv 17 \equiv 8 \pmod 9$, and so $234785346 \cdot 5683592187 \not\equiv 1334424157147691702$. (In fact, $234785346 \cdot 5683592187 = 133442415\underline{8}147691702$).

[4] 5. (a) The binary expansion of 18 is $18 = 16 + 2 = 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$, so here $r = 4$ and $i_1 = i_2 = i_4 = 0$, $i_3 = 1$. Thus, the power-mod algorithm runs as follows:

$$\begin{array}{lll|lll} y_0 & \equiv & 5 \pmod{11} & y_3 & \equiv & y_2^2 a^{i_3} \equiv (-2)^2 5 \equiv -2 \pmod{11} \\ y_1 & \equiv & y_0^2 a^{i_1} \equiv 5^2 \equiv 3 \pmod{11} & y_4 & \equiv & y_3^2 a^{i_4} \equiv (-2)^2 \equiv 4 \pmod{11} \\ y_2 & \equiv & y_1^2 a^{i_2} \equiv 3^2 \equiv -2 \pmod{11} & & & \end{array}$$

Thus, $\mathrm{rem}(5^{18}, 11) = 4$.

(b) Similarly, since $14 = 8 + 6 = 8 + 4 + 2 = 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$, we have here $r = 3$ and $i_1 = i_2 = 1$, $i_3 = 0$. Thus, $\mathrm{rem}(7^{14}, 18) = 13$ because

$$\begin{array}{lll|lll} y_0 & \equiv & 7 \pmod{18} & y_2 & \equiv & y_1^2 a^{i_2} \equiv 1^2 \cdot 7 \equiv 7 \pmod{18} \\ y_1 & \equiv & y_0^2 a^{i_1} \equiv 7^2 \cdot 7 \equiv (-5)7 \equiv 1 \pmod{18} & y_3 & \equiv & y_2^2 a^{i_3} \equiv 7^2 \equiv 13 \pmod{18}. \end{array}$$

[4] 6. See the MAPLE solution on the course Web site (www.mast.queensu.ca/~math211).