Name: ID#: Serial #:

---

1. [10pts] (a) Reduce the congruence $x^{10}+x^7+3x^4 \equiv 2 \pmod 5$ to an equivalent congruence of degree at most 4.

Solution

$$x^{10}+x^7+3x^4 = \left(x^5-x\right)\left(x^5+x\right)+\left(x^5-x\right)x^2+3x^4+x^3+x^2$$

Hence $x^{10}+x^7+3x^4 \equiv 2 \pmod 5$ is equivalent to $3x^4+x^3+x^2 \equiv 2 \pmod 5$.

(b) Show that $x^{12}+10x^2 \equiv 0 \pmod{11}$ has 11 solutions.

Proof. $x^{12}+10x^2 \equiv 0 \pmod{11}$ is equivalent to $(x^{11}-x)\,x \equiv 0 \pmod{11}$. By Fermat's theorem, $x^{11}-x \equiv 0 \pmod{11}$ has 11 solutions, so the given congruence also has 11 solutions (which is therefore an identical congruence).

---

2. [15pts] (a) Find a primitive root mod 29.

Solution. $\varphi(29)=28$, with prime divisors 2 and 7. We have

$$\begin{aligned} 2^4 &\equiv 16 \not\equiv 1 \pmod{29} \\ 2^{14} &\equiv \left(2^5\right)^2 2^4 \equiv 3^2(-13) \equiv 3\times(-39) \equiv -30 \not\equiv 1 \pmod{29} \end{aligned}$$

so 2 is a primitive root mod 29.
[3 is also a primitive root mod 29 and is slightly simpler to test because $3^3 \equiv -2 \pmod{29}$.]

(b) Determine the number of solutions of the congruence $x^{12} \equiv 7 \pmod{29}$.

Solution. Since 29 is prime, we first check if $7^{\frac{28}{(12,28)}} \equiv 1 \pmod{29}$. We have

$$7^{\frac{28}{(12,28)}} = 7^7 = \left(7^2\right)^3 \times 7 \equiv \left(-9^2\right) \times 63 \equiv 6 \times 5 \equiv 1 \pmod{29}$$

Hence the given congruence has $(12,28)$, i.e. 4, solutions.

(c) Let p be prime and such that $p \equiv 3 \pmod 4$ and let g be a primitive root mod p. Prove that $-g$ is not a primitive root mod p.

Proof. Since g is a primitive root mod p and $\left(g^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p$, we obtain $g^{\frac{p-1}{2}} \equiv -1 \pmod p$. Also, since $p \equiv 3 \pmod 4$, we obtain $(-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$. Hence

$$(-g)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} g^{\frac{p-1}{2}} \equiv 1 \pmod p$$

so that $-g$ is not a primitive root mod p. ■

---

3. [15pts] (a) State the quadratic reciprocity law and determine whether the congruence

$$x^2 \equiv 21 \pmod{89}$$

is solvable.

Solution. *QRL*: If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

We have $\left(\frac{21}{89}\right) = \left(\frac{10^2}{89}\right) = 1$. Hence the given congruence is solvable.

(b) Determine if the congruence $x^2 + 6x - 2 \equiv 0 \pmod{67}$ is solvable.

Solution. We have $x^2 + 6x - 2 = (x+3)^2 - 11$. Also, 11 and 67 are primes both congruent to 3 mod 4, hence $\left(\frac{11}{67}\right) = -\left(\frac{67}{11}\right) = -1$. So the given congruence is not solvable.

(c) Prove that if p is an odd prime, then $\left(\frac{(p+1)/2}{p}\right) = (-1)^{(p^2-1)/8}$

Solution. We have $1 = \left(\frac{p+1}{p}\right) = \left(\frac{(p+1)/2}{p}\right)\left(\frac{2}{p}\right)$, hence $\left(\frac{(p+1)/2}{p}\right) = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

---

4. [10pts] (a) Find the highest power of 20 dividing 300!

Solution. The highest power of 20 dividing 300! is that of 5, which is

$$\left[\frac{300}{5}\right] + \left[\frac{300}{5^2}\right] + \left[\frac{300}{5^3}\right] = 60 + 12 + 2 = 74$$

Hence the highest power of 20 dividing 300! is 20^{74}.

(b) Prove that for any positive real numbers x, y we have $[x][y] \le [xy] \le [x][y] + [x] + [y]$. Is it possible to find a real number z such that $[z]^2 = [z^2] + 2$? Justify.

Proof. Since $[x] \le x < [x]+1$, $[y] \le y < [y]+1$, and $x, y > 0$, we get $[x][y] \le xy$, hence $[x][y] \le [xy]$. Also, $[xy] \le xy < ([x]+1)([y]+1) = [x][y] + [x] + [y] + 1$, so that $[xy] \le [x][y] + [x] + [y]$.

Another way: Let $x = [x] + \varepsilon$, $y = [y] + \delta$ (so that $0 \le \varepsilon, \delta < 1$). We have

$$[xy] = [([x]+\varepsilon)([y]+\delta)] = [[x][y] + \delta[x] + \varepsilon[y] + \varepsilon\delta] = [x][y] + [\delta[x] + \varepsilon[y] + \varepsilon\delta]$$

Hence $[xy] \ge [x][y]$ $(\because \delta[x] + \varepsilon[y] + \varepsilon\delta \ge 0)$, and

$$\begin{aligned} [xy] &\le [x][y] + [[x] + [y] + \varepsilon\delta] \quad (\because \delta[x] \le [x],\ \varepsilon[y] \le [y]) \\ &= [x][y] + [x] + [y] + [\varepsilon\delta] = [x][y] + [x] + [y] \quad (\because 0 \le \varepsilon\delta < 1) \end{aligned}$$

For the last question, take $z = -1.5$. Then $[z]^2 = 4 = [z^2] + 2$. (Of course, by the previous part, such z cannot be positive.)
