Problem 3.21

1. n = 1739

22! – 1 = 3 (mod 1739) GCD(3, 1739) = 1

23! – 1 = 63 (mod 1739) GCD(63, 1739) = 1

24! – 1 = 1082 (mod 1739) GCD(1082, 1739) = 1

25! – 1 = 1394 (mod 1739) GCD(1394, 1739) = 1

26! – 1 = 1443 (mod 1739) GCD(1443, 1739) = 37

1739 / 37 = 47

(37 – 1) = 36 = 22 \* 33

Factors are 37 and 47, 37 has the property that p – 1 is a product of small primes

1. n = 220459

22! – 1 = 3 (mod 220459) GCD(3, 220459) = 1

23! – 1 = 63 (mod 220459) GCD(63, 220459) = 1

24! – 1 = 22331 (mod 220459) GCD(22331, 220459) = 1

25! – 1 = 85053 (mod 220459) GCD(85053, 220459) = 1

26! – 1 = 4045 (mod 220459) GCD(4045, 220459) = 1

27! – 1 = 43102 (mod 220459) GCD(43102, 220459) = 1

28! – 1 = 179600 (mod 220459) GCD(179600, 220459) = 449

220459 / 449 = 491

(449 – 1) = 448 = 26 \* 7

Factors are 449 and 491, 449 has the property that p – 1 is a product of small primes

1. n = 48356747

22! – 1 = 3 (mod 220459) GCD(3, 48356747) = 1

23! – 1 = 63 (mod 220459) GCD(63, 48356747) = 1

24! – 1 = 16777215 (mod 220459) GCD(16777215, 48356747) = 1

25! – 1 = 29007255 (mod 220459) GCD(29007255, 48356747) = 1

26! – 1 = 6497325 (mod 220459) GCD(6497325, 48356747) = 1

27! – 1 = 11540769 (mod 220459) GCD(11540769, 48356747) = 1

28! – 1 = 13320679 (mod 220459) GCD(13320679, 48356747) = 1

29! – 1 = 2119446 (mod 220459) GCD(2119446, 48356747) = 1

210! – 1 = 32129513 (mod 220459) GCD(32129513, 48356747) = 1

211! – 1 = 4931911 (mod 220459) GCD(4931911, 48356747) = 1

212! – 1 = 35410323 (mod 220459) GCD(35410323, 48356747) = 1

213! – 1 = 46845550 (mod 220459) GCD(46845550, 48356747) = 1

214! – 1 = 45774460 (mod 220459) GCD(45774460, 48356747) = 1

215! – 1 = 46983890 (mod 220459) GCD(46983890, 48356747) = 1

216! – 1 = 8398520 (mod 220459) GCD(8398520, 48356747) = 1

217! – 1 = 9367159 (mod 220459) GCD(9367159, 48356747) = 1

218! – 1 = 17907955 (mod 220459) GCD(17907955, 48356747) = 1

219! – 1 = 13944672 (mod 220459) GCD(13944672, 48356747) = 6917

48356747 / 6917 = 6991

(6917 – 1) = 6916 = 22 \* 7 \* 13 \* 19

Factors are 6917 and 6991, 6917 has the property that p – 1 is a factor of small primes