1.33(b)
1.37
1.38

Simon Owens Crypto

$10 \bmod 5 = 0$
$7 \bmod 5 = 2$

$5\overline{)\,7}$ 1, 5, 2

1.33(b)

We are trying to figure out how many times we must run. Let $g \in \mathbb{F}_p^*$ be a primitive root. If this is true, then every $a \in \mathbb{F}_p^*$ form is g^i for some $0 \le i < p-1$.

We know $a^{\frac{(p-1)}{q}} = 1$

so

plug in g^i for a

$$\#\{a \in \mathbb{F}_p^* : a^{\frac{(p-1)}{q}} = 1\} = \#\{0 \le i < p-1 : (g^i)^{\frac{(p-1)}{q}} = 1\}$$
$$= \#\{0 \le i < p-1 : g^{i\frac{(p-1)}{q}} = 1\}$$

$$g^{i\left(\frac{p-1}{q}\right)} = 1 \Leftrightarrow p-1 \text{ or } \frac{i(p-1)}{q} \Longleftrightarrow \frac{q}{i}$$

$$\text{So } \#\{a \in \mathbb{F}_p^* : a^{\frac{(p-1)}{q}} = 1\} = \#\{0 \le i < p-1 : q / i\} = \frac{p-1}{q}$$

As a result

$$\#\{a \in \mathbb{F}_p^* : a^{\frac{(p-1)}{q}} \ne 1\} = p-1 - \#\{a \in \mathbb{F}_p^* : a^{\frac{(p-1)}{q}} = 1\}$$
$$= p-1 - \frac{p-1}{q} = (p-1)\left(1 - \frac{1}{q}\right)$$

Since we found that we ~~take it equal to~~ what was previously stated

$$\boxed{\frac{\#\{a \in \mathbb{F}_p^* : a^{\frac{(p-1)}{q}} \ne 1\}}{\#\mathbb{F}_p^*} = 1 - \frac{1}{q}}$$

If q is a super large number then we would probably get it quickly

Simon Owens
Cryptography

1.38

$2^{\frac{(p-1)}{2}} \pmod p \qquad 3 \le p \le 20$

Solving

$p=3 \quad 2^1 = 2 \equiv 2$

$p=5 \quad 2^2 = 4 \equiv 4$

$p=7 \quad 2^3 = 8 \equiv 1$

$p=11 \quad 2^5 = 32 \equiv 10$

$p=13 \quad 2^6 = 64 \equiv 12$

$p=17 \quad 2^8 = 256 \equiv 1$

$p=19 \quad 2^9 = 512 \equiv 18$

The conjecture is that $2^{\frac{(p-1)}{2}} \equiv 1$ or $p-1 \bmod p$.
We need to prove p divides $\underline{a-1}$ or $\underline{a+1}$.

$a = 2^{\left(\frac{p-1}{2}\right)}$, Using Fermat's theorem gives us $a^2 \equiv 2^{p-1} \equiv 1$

So this tells us $a \equiv \pm 1 \pmod p$. As a result

$\frac{p}{(a^2-1)}$ gives us $\longrightarrow \boxed{\frac{p}{(a-1)(a+1)}}$

$\downarrow$

$\boxed{a \equiv \pm 1 \bmod p}$